2/2022

DVD Deutsche Vereinigung für Datenschutz e.V.

Datenschutz Nachrichten

45. Jahrgang
ISSN 0137-7767
14,00 Euro



Social Media

■ Google-Tools für Webseiten und datenschutzfreundliche Alternativen ■ Cookies – Spuren im Netz ■ Betroffen von Datenschutzverstößen – Was tun? ■ Tipps im Internet zur datenschutzgerechten Nutzung sozialer Medien ■ Europa reguliert mit dem Digital Services Act das Internet ■ BigBrotherAwards 2022 ■ Pressemitteilungen ■ Nachrichten ■ Rechtsprechung ■ Buchbesprechungen ■

Deutsche Vereinigung für Datenschutz e.V.
www.datenschutzverein.de

Inhalt

Termine



Foto: Pixabay..com

Montag, 01.08.2022
Redaktionsschluss DANA 3/2022
Schwerpunkt: Datenschutz als Grundrecht

Sonntag, 11.09.2022
DVD-Vorstandssitzung
Kiel

Montag, 12.09.2022
Sommerakademie 2022
ULD, Kiel

Freitag, 23.09.2022
Datenschutztag 2022
Computas, Köln

Mittwoch/Donnerstag, 28./29.09.2022,
Privacy Conference
Bitkom, online

Donnerstag/Freitag, 13./14.10.2022
Jahreskonferenz
Forum Privatheit, Berlin

Samstag, 22.10.2022
DVD-Vorstandssitzung
Bonn

Mittwoch/Donnerstag, 26./27.10.2022,
Herbstkonferenz
BvD, Stuttgart

Freitag, 28.10.2022
Behördentag
BvD, Stuttgart

DANA
Datenschutz Nachrichten
ISSN 0137-7767
45. Jahrgang, Heft 2

Herausgeber
Deutsche Vereinigung für Datenschutz e.V. (DVD)
DVD-Geschäftsstelle:
Reuterstraße 157, 53113 Bonn
Tel. 0228-222498
IBAN: DE94 3705 0198 0019 0021 87
Sparkasse KölnBonn
E-Mail: dvd@datenschutzverein.de
www.datenschutzverein.de

Redaktion (ViSdP)
Hans-Dieter Neumann
c/o Deutsche Vereinigung für Datenschutz e.V. (DVD)
Reuterstraße 157, 53113 Bonn
dvd@datenschutzverein.de
Den Inhalt namentlich gekennzeichneter Artikel verantworten die jeweiligen Autorinnen und Autoren.

Layout und Satz
Frans Jozef Valenta, 53119 Bonn
valenta@datenschutzverein.de

Druck
Onlineprinters GmbH
Dr.-Mack-Straße 83
90762 Fürth
www.onlineprinters.de
Tel. +49 (0) 9161 6209800
Fax +49 (0) 9161 8989 2000

Bezugspreis
Einzelheft 14 Euro. Jahresabonnement 48 Euro (incl. Porto) für vier Hefte im Jahr. Für DVD-Mitglieder ist der Bezug kostenlos. Nach einem Jahr kann das Abonnement jederzeit mit einer Frist von einem Monat gekündigt werden. Die Kündigung ist schriftlich an die DVD-Geschäftsstelle in Bonn zu richten.

Leserbriefe
Leserbriefe sind erwünscht. Deren Publikation sowie eventuelle Kürzungen bleiben vorbehalten.

Abbildungen, Fotos
Frans Jozef Valenta, Pixabay, iStock,
Titel: iStock/...

Editorial

Der Schwerpunkt dieser Datenschutz Nachrichten beschäftigt sich mit Social Media und dem Problem des Tracking. Dazu haben wir uns einen großen Dienstleister im Internet mit seinem datengetriebenen Geschäftsmodell angeschaut (Klaus Meffert). Ergänzend werden auch alternative Produkte besprochen. In einem Podcast, den wir freundlicherweise überarbeiten und in Textform darstellen durften, werden Cookies, ihre Funktion und mögliche Abwehrmechanismen erläutert, einschließlich der Folgen, die das für Betroffene haben kann. Auch hier gibt es Alternativen.

Eine Autorin (Name der Redaktion bekannt) schreibt uns ihre Begründung dafür, dass sie allen bekannten Datenschutzhinweisen zum Trotz Facebook verwendet. Da bleibt es nicht aus, dass man irgendwann selbst von Datenschutzverstößen betroffen ist. Was dann zu tun ist, erläutert Thilo Weichert. Die Betroffenenrechte sind recht umfassend ausgestaltet und verlangen eine intensive Beschäftigung mit dem Kapitel III der DSGVO. Diese Hinweise werden ergänzt durch den Aufsatz zur datenschutzgerechten Mediennutzung von Heinz Alenfelder. Er stellt unter anderem auch die Möglichkeiten vor, die uns das BSI und andere Akteure zur Verfügung stellen. Frans Valenta informiert uns über technische Innovationen aus China. Er präsentiert zwei technisch hervorragende Produkte aus dem Reich der Mitte, deren Anwendungen jedoch viel Raum für Datenschutzmaßnahmen eröffnen.

Katrin Lowitz setzt sich mit den Nutzungs- und anderen Bedingungen in der Social-Media-Welt auseinander und liefert daneben einen Abriss der geschichtlichen Entwicklung von der Gründungszeit der sozialen Medien bis hin zu den politischen Einflussmöglichkeiten, die heutzutage möglich sind. Einen hochaktuellen Beitrag zum Digital Services Act liefert Klaus-Jürgen Roth. Dieses Gesetz sowie weitere werden wir in den nächsten DANA-Ausgaben eingehender besprechen.

Auch in diesem Jahr haben die datenschutzrechtlich besonders schlecht ausgestatteten Organisationen ihren Preis bekommen. Wir berichten über die „Oscars für Datensünder“ und müssen feststellen, dass selbst Sicherheitsorgane zu den Preisträgern gehören. Nachrichten, Urteile und Buchbesprechungen sowie ein Leserbrief runden das Angebot dieser DANA-Ausgabe ab. Ich wünsche Ihnen eine angenehme und anregende Lektüre.

Ihre DANA-Redaktion

Autorinnen und Autoren dieser Ausgabe:

Heinz Alenfelder, Vorstandsmitglied der DVD, alenfelder@datenschutzverein.de

K.P. (Name der Redaktion bekannt), private Nutzerin von Social Media

Katrin Lowitz, Journalistin, info@beyond-eve.com

Dr. Ing. Klaus Meffert, Informatiker und Datenschützer, klaus.meffert@dr-dsgvo.de

Hans-Dieter Neumann, Datenschutzbeauftragter und Vorstandsmitglied der DVD, neumann@datenschutzverein.de

Klaus-Jürgen Roth, Bonn, dvd@datenschutzverein.de

Frans Josef Valenta, Vorstandsmitglied der DVD, valenta@datenschutzverein.de

Dr. Thilo Weichert, Vorstandsmitglied der DVD, Netzwerk Datenschutzexpertise, weichert@datenschutzverein.de

Ira Zahorsky, Redakteurin, ira.zahorsky@vogel.de

Klaus Meffert

Google-Tools für Webseiten und datenschutzfreundliche Alternativen

Wie Google Daten sammelt und warum das problematisch sein kann

Einleitung

Bei vielen Betreibern von Webseiten sind die kostenfrei verfügbaren Google-Dienste beliebt. Beispielsweise kann mit einem Plugin eine **interaktive Karte** eingebunden werden. Auch **Schriftarten**, die von Google bereitgestellt werden, werden oft genutzt. Weitere Tools, wie diese Dienste oder Plugins auch genannt werden, runden das Angebot ab. Dazu zählen beispielsweise **Google reCAPTCHA** zum Absichern von Formularen und Webseiten oder **Google Analytics** zum Analysieren von Nutzern auf verschiedene Weise.

So sehr die Google-Dienste mit ihrer Funktionalität bestechen, so problematisch sind sie doch zu beurteilen, wenn es um den Datenschutz geht. Die Gründe dafür beschreibe ich nachfolgend.

Mutterkonzern in den USA

Google hat bekanntlich seine Wurzeln in den USA. Die weltweit agierenden Google-Töchter hängen alle an amerikanischen Muttergesellschaften.

Seit dem Urteil des Europäischen Gerichthofs (EuGH) sind Datenübertragungen in die USA hochproblematisch. Das bezieht sich auch auf die Möglichkeit von den USA aus auf die Daten zugreifen zu können.

Das Urteil wurde von Max Schrems erwirkt und heißt deswegen „Schrems II". Der EuGH hat den sogenannten Privacy Shield für ungültig erklärt. Der Privacy Shield war ein informelles Datenschutzabkommen zwischen Europa und den USA. Das erste Urteil, welches Schrems zuvor erwirkte, erklärte das frühere Datenschutzabkommen namens „Safe Harbor" für ungültig.

Aktuell ist ein neues Datenschutzabkommen zwischen der EU und den USA im Gespräch. Solange die im folgenden genannten Überwachungsgesetze allerdings in Kraft sind, wird es keine Aussicht auf Erfolg haben und spätestens mit dem nächsten EuGH-Urteil für nichtig erklärt.

Überwachungsgesetze in den USA

Worum geht es beim Schrems-II-Urteil und warum ist Datenschutz in den USA so kritisch zu bewerten?

Die USA erlauben es Behörden und Geheimdiensten aufgrund von Verfahren, die nicht den Standards des europäischen Rechtsverständnisses genügen, die Daten von deutschen und anderen europäischen Bürgern abzugreifen. Für die interessierten Leser, die sich weiter informieren möchten, sind hier die Überwachungsgesetze EO 12333, FISA 702 und Cloud Act genannt.

Das Problem ist, dass betroffene Personen aus Europa naturgemäß nichts davon erfahren überwacht zu werden. Die DSGVO garantiert den Betroffenen aber, dass sie dies erfahren dürfen und dass ihre persönlichen Daten geschützt sind. Unter anderem deswegen kann die DSGVO in den USA nicht eingehalten werden.

Serverstandort egal

Die Überwachungsgesetze der USA gelten unabhängig vom Standort eines Servers. Bietet eine amerikanisch geführte Firma einen Service an, der Server nutzt, die sich in Europa befinden, können amerikanische Behörden über die US-Überwachungsgesetze dennoch auf diese Server zugreifen. Hierzu wird die amerikanische Muttergesellschaft aufgefordert die Daten auf dem Server, auf den sie technisch oder rechtlich Zugriff haben kann, herauszugeben. Die Muttergesellschaft hat dann zur Not eine ihrer Tochtergesellschaften aufzufordern sie dabei zu unterstützen.

Personenbezug bei Webseitenbesuch

Die DSGVO regelt ausdrücklich die Nutzung solcher Daten, die direkt oder indirekt einer Person zugeordnet werden können oder aufgrund derer eine Person identifiziert werden kann.

Besucht jemand eine Webseite, wird aus technischen Gründen dabei immer die **Netzwerkadresse** des Besuchers übermittelt. Diese Netzwerkadresse heißt auch IP-Adresse. Die IP-Adresse gilt als personenbezogenes Datum. Das wurde 2016 vom EuGH grundsätzlich festgestellt und vom Bundesgerichtshof (BGH) 2017 für Deutschland bestätigt.

Bindet eine Webseite nun ein Google-Plugin ein, etwa zur Anzeige einer interaktiven Karte, dann wird die Netzwerkadresse des Besuchers der Webseite aus technisch notwendigen Gründen auch an Google übertragen.

Somit findet eine Übertragung personenbezogener Daten derart statt, dass über amerikanische Überwachungsgesetze ein Zugriff darauf in einer mit der DSGVO nicht vereinbaren Weise möglich ist.

Verhaltensanalyse durch Google

Das Geschäftsmodell von Google ist stark datengetrieben. Ein großer Teil des riesigen Umsatzes wird mit personalisierter Werbung erwirtschaftet. Damit Google Werbung personalisieren kann, müssen Nutzer besser kennengelernt werden.

Dazu analysiert Google das Verhalten von Ihnen und mir, Ihre Surfgewohnheiten und Vorlieben. Technisch ist es für einen weltweit genutzten Konzern leicht möglich Ihre Reise durch das Internet sehr genau nachzuzeichnen. Das Android-Smartphone und die Google-Suchmaschine sind zwei Kontaktpunkte, die Google besonders viele ergiebige Daten liefern dürften.

Die Daten, die Google erhält, stammen teils aus eigenen Erhebungen, wie bei der Google-Suchmaschine oder Android-Smartphones. Aber auch Webseiten, die Google-Plugins installiert haben, senden Signale von Ihnen an Google, wenn Sie die entsprechende Webseite besuchen. Diese Datenerfassung finden in vielen Fällen ohne Rechtsgrundlage statt. Verantwortlich ist derjenige, der die gerade besuchte Webseite betreibt, auch wenn derjenige oft selbst nichts davon hat, dass Google Ihre Daten erhält. Google selbst nutzt bis dato Einwilligungsabfragen, die nicht rechtskonform sind, wie kürzlich verschiedene europäische Datenschutzbehörden feststellten.

Oft nutzt Google auch Cookies, um Nutzer möglichst eindeutig zu identifizieren. Diese Cookies sind oft nicht einwilligungsfrei, werden aber ohne ordentliche Einwilligung verwendet. Das nur am Rande. Wer mehr wissen will, findet in § 25 TTDSG einen Anhaltspunkt.

Mögliche Abhilfe

Bei standardisierten Tools und Plugins wie denen von Google kann keine Verschlüsselung von Nutzerdaten, wie der Netzwerkadresse, vorgenommen werden. Die Verschlüsselung wäre ansonsten ein Mittel, um die Nutzerdaten ausreichend zu schützen und die Probleme mit Überwachungsgesetzen zu beseitigen.

Die DSGVO bietet als Rechtsgrundlage bei (potentieller) Datenverarbeitung in einem unsicheren Drittland die Einwilligung durch einen Nutzer an. Dies steht in Art. 44ff DSGVO. Die Einwilligung kann vom Betreiber einer Webseite grundsätzlich eingeholt werden, bevor die Webseite einen Google-Dienst einbettet.

Die Einwilligungsabfrage für Google-Plugins ist allerdings kaum (oder gar nicht) in rechtskonformer Weise möglich. Denn dazu müsste der Webseitenbetreiber als Verantwortlicher alles über die Datenverarbeitung wissen, was auch Google weiß. Google verrät allerdings nur in eingeschränkter und intransparenter Weise, was mit den Daten passiert, die Google von anderen erhält.

Demnach ist selbst eine Einwilligungsabfrage für Google-Plugins keine wirklich rechtssichere Möglichkeit. Dies stellte auch die französische Datenschutzbehörde CNIL für Google Analytics Anfang 2022 fest und verbot dieses Tracking-Tool gänzlich.

Datenschutzfreundliche Möglichkeiten

Je nachdem, was Sie als Webseitenbetreiber erreichen möchten, gibt es unterschiedliche Möglichkeiten, um auf Google-Dienste zu verzichten.

Vorteile

Der Verzicht auf den Einsatz von Diensten amerikanischer Unternehmen hat mehrere Vorteile.

Erstens **sparen Sie** im Endeffekt eine Menge **Aufwand**. Der Aufwand für das Installieren eines alternativen Plugins mag höher sein als für die funktionell perfekt durchgestylten Google-Plugins. Aber der Aufwand für die Abstimmung mit einem Datenschutz-Experten oder dem Webseiten-Betreuer ist erheblich geringer.

Zweitens benötigen Sie **keine Einwilligungsabfrage**, die auch als Cookie-Popup benötigt wird. Sicher wurden Sie selbst schon mehrfach von solchen Popups belästigt und fanden diese einfach nur nervig. Genauso geht es Besuchern Ihrer Webseite auch, wenn dort ein Cookie-Popup weggeklickt werden muss. Wer kein Popup braucht, muss es auch nicht installieren und konfigurieren oder jemanden beauftragen, das zu tun.

Drittens erhöhen Sie so Ihre **Rechtssicherheit** erheblich. Meine Untersuchungen zeigen, dass Cookie-Popups in der Praxis sehr oft zu rechtswidrigen Webseiten führen oder gerade der Grund für die Probleme sind. Hierfür gibt es **mehrere Gründe**, die ich einem eigenen Artikel[1] beschreibe.

Lösungen

Für einige häufige Anwendungsfälle finden Sie nun Empfehlungen für datenschutzfreundliche Lösungen. Als Aufhänger ist das jeweilige Google-Tool genannt, das dadurch ersetzt werden kann.

Google-Maps-Plugin

Zweck: Interaktive Karte auf einer Webseite einbetten, meist zur Anzeige eines Standorts.

Oft möchten Sie vielleicht tatsächlich einen **Standort anzeigen**. In diesem Fall empfehle ich eine interaktive Karte auf Basis von OpenStreetMap (OSM).

OpenStreetMap ist wesentlich datenschutzkonformer als Google Maps. Jedoch sollten Sie OpenStreetMap nicht direkt einbetten, damit die Daten Ihrer Nutzer nicht an die Anbieter von OpenStreetMap geschickt werden und Sie nicht in Erklärungsnot geraten.

Mein Plugin[2] für eine interaktive Karte bietet vollen Datenschutz. Die Daten Ihrer Nutzer werden nicht weitergegeben. Eine Cookie-Popup ist nicht nötig.

Wenn Sie hingegen Ihren Besuchern eine **Anfahrtsplanung** ermöglichen möchten, empfehle ich statt dessen einen Button mit der Aufschrift „Anfahrt planen“. Haben Sie kaum Publikumsverkehr, dann brauchen Sie vielleicht weder eine interaktive Karte noch einen solchen Button.

Möchten Sie zeigen, wo sich Ihr Unternehmen befindet, ist oft eine reizvolle **Umgebungskarte** oder Standortkarte als statisches Bild nützlicher. Ein solches Bild gibt es vielleicht von Ihrem Stadtmarketing oder kann selbst angefertigt werden. Ja, das ist mehr Aufwand, als ein nur wenig reizvolles, vorgefertigtes Kartenmaterial einzubinden, ist aber sinnvoller.

Google Fonts

Zweck: Schriftart nutzen.

Google Fonts werden auch als Google Web Fonts oder Google Schriften bezeichnet.

In Wahrheit bietet Google „nur“ eine Infrastruktur, über die Designer ihre selbst erstellten Schriften hochladen und Sie diese Schriften auf Ihrer Webseite abrufen können.

Werden die Schriften von einem Google-Server abgerufen, ist dies laut LG München (Urteil vom 20.01.2022 – 3 O 17493/20) rechtswidrig. Ich selbst hatte das schon ein Jahr vorher festgestellt. Der wichtigste Grund ist aus meiner Sicht das Vorhandensein eines **milderen Mittels**.

Sie können die Schriften **lokal einbinden** anstatt sie vom Google Server zu laden. Das ist technisch möglich und lizenzrechtlich erlaubt. Für die lokalen Schriften benötigen Sie **keinen Datenschutztext**.

Das Tool **Google Web Fonts Helper** erlaubt es Schriften herunterzuladen. Danach können die Schriften auf den eigenen Webserver kopiert und von dort eingebunden werden. Den Link zum Tool finden Sie in meinem Beitrag zu Google Fonts[3]. Dort nenne ich auch Argumente, die das eben genannte Urteil des LG München stützen.

Google reCAPTCHA

Zweck: Formular vor Spam schützen.

Mit reCAPTCHA werden oft Formulare gegen Spam abgesichert. Damit soll verhindert werden, dass Computerprogramme, sogenannte Bots, automatisiert ein Formular ausfüllen und Sie deswegen eine **unerwünschte Nachricht** erhalten.

reCAPTCHA von Google nutzt zahlreiche Cookies und ist deshalb rechtlich kaum beherrschbar. Auch der USA-Bezug, den ich oben erwähnt hatte, lässt sich nicht wegdiskutieren.

Mit einem **zusätzlichen Formularfeld** können Sie die meisten Roboter aussperren. Stellen Sie eine **einfache Rechenaufgabe**, die ein Mensch leicht lösen kann, ein Roboter aber nicht. Im Eingabefeld dazu ist die Lösung einzugeben. Nur wenn die Lösung richtig ist, kann das Formular abgeschickt werden.

Fragen Sie beispielsweise: „Wie viel sind neun weniger 2? Ergebnis bitte als Wort schreiben".

Wer technisch versierter ist, kann statt dessen eine auf der **Programmiersprache PHP** basierende Lösung einbinden. PHP ist eine universell nutzbare Sprache, die fast jeder Webserver versteht.

Für **WordPress-Webseiten** gibt es das Plugin Contact Form 7 Image Captcha[4]. Es stellt vier Symbole dar und fragt „Klicken Sie auf das Auto".

Google Analytics

Zweck: Verhalten von Nutzern analysieren.

Meistens wird Google Analytics zur Reichweitenmessung verwendet. Oder das Tool wird nach meiner Erfahrung gar nicht genutzt und ist nur deshalb noch eingebunden, weil es noch nicht entfernt wurde.

Um zu wissen, wie viele Besucher Ihre Webseite hat, können Sie zahlreiche Lösungen nutzen, die keine Einwilligungsabfrage erfordern und von Ihnen selbst betrieben werden. Hier ein paar Beispiele:

- Matomo[5]: kostenfrei, Open Source, lokal installierbar.
- WP Statistics[6]: kostenfrei, Open Source, lokal, für WordPress.
- Offen.dev[7]: kostenfrei, Open Source.
- Conversion Tracking[8]: Auch datenschutzkonform möglich.

Sie erfahren damit auch, welche Ihrer Seiten am meisten aufgerufen werden und von wo die Besucher kamen (beispielsweise: Suchmaschine X oder Direktaufruf).

Google Search Console

Zweck: Ermitteln, mit welchen Suchbegriffen die eigene Webseite gefunden wurde.

Eine gute Nachricht zum Schluss: Dieser Google-Dienst kann weiterhin genutzt werden. Es handelt sich um eine eigenständige Funktionalität außerhalb Ihrer Verantwortlichkeit. Google ermittelt über die in der Google Suchmaschine präsentierten Suchergebnisse eigenverantwortlich, welche Suchbegriffe zu einem Treffer für Ihre Webseite führten.

Sie müssen dafür nichts auf Ihrer eigenen Webseite installieren, sondern sich lediglich bei der Google Search Console registrieren. Übrigens gibt es etwas ähnliches auch bei anderen Suchmaschinen, wie Bing von Microsoft (Bing Webmaster Tools).

Wenn wir schon bei Suchmaschinen sind. Vielleicht möchten Sie einmal duckduckgo.com oder ecosia.org ausprobieren? Statt dem Chrome Browser von Google könnten Sie Firefox oder auf dem Handy den Browser von duckduckgo nutzen.

Fazit

Für nahezu jedes häufige Problem gibt es eine datenschutzfreundliche Alternative.

Der Gesamtaufwand für die Installation solcher Alternativen auf Webseiten ist nach meiner Erfahrung geringer als die Nutzung von leicht zugänglichen Tools und Plugins.

Rechtssicherheit muss eben mit eingepreist werden. Wer sich vorgenommen hat aufgrund von Datenschutzvorfällen, Gesetzesänderungen, neuen Gesetzen oder wegen der Berichterstattung über Abmahnungen tätig zu werden, kann es auch gleich richtig machen und muss nicht auf eine Motivation von außen warten.

Cookie-Popups können vermieden werden, wenn Lösungen eingesetzt werden, die keine Datenschutzprobleme erzeugen. Der Effekt dürften weniger genervte und somit zufriedenere Nutzer sein, die eher Umsatz bringen.

Die DSGVO hat nicht wirklich viel Neues eingeführt, wenn man sich das Vorgängergesetz, das Bundesdatenschutzgesetz, ansieht. Auch das Urteil zu IP-Adressen wurde vor der DSGVO gesprochen. Wenn Internetkonzerne Datenschutz ernster nehmen würden, hätten wir viel weniger Probleme, um die wir uns kümmern müssten.

Nutzen Sie den Datenschutz als Qualitätsmerkmal und sehen Sie ihn als Möglichkeit zur Effizienzsteigerung und für einen ruhigeren Schlaf. Immerhin haben deutsche und europäische Unternehmen die Chance mit datenschutzfreundlichen Lösungen zu punkten und auf dem Markt zu bestehen.

Oft ist weniger mehr. Nicht alles, was möglich ist, ist sinnvoll. Ich konnte hier nicht auf weitere Aspekte eingehen, wie etwa Online Werbung. Auch hier gilt das, was mir meine Lebenserfahrung aus dem Geschäftsleben zeigt: Der einfachste Weg ist meist nicht der optimale. Das, was alle tun, ist oft nicht der beste Weg. Kostenlos bedeutet oft im wahrsten Sinne des Wortes umsonst.

1. https://dr-dsgvo.de/cookie-popups-darum-funktionieren-sie-nicht/
2. https://dr-dsgvo.de/karte
3. https://dr-dsgvo.de/google-schriften-auf-websites-nur-mit-einwilligung/
4. https://wordpress.org/plugins/contact-form-7-image-captcha/
5. Konfigurationshinweise unter https://dr-dsgvo.de/matomo-fuer-besucher-statistiken-auf-webseiten-datenschutzkonform-und-ohne-einwilligung-nutzen/
6. https://de.wordpress.org/plugins/wp-statistics/
7. https://www.offen.dev/
8. Hinweise unter: https://dr-dsgvo.de/conversion-tracking-und-marketing-attribution-auf-webseiten-datenschutzfreundlich-moeglich/

Cookies – Spuren im Netz

Ein Podcast der Vogel IT-Medien GmbH, moderiert von Ira Zahorsky. Gesprächspartner ist Hans-Dieter Neumann (DVD). Der gesprochene Text wurde für den Druck überarbeitet. Der Podcast ging am 07.06.2022 online.[1]



Bild: iStock.com/ klyaksun

Intro: Online-Werbung ist überall und ein Riesengeschäft. Um personalisierte Werbung ausspielen zu dürfen, müssen die User einer Website den Cookies zustimmen. Das ist normalerweise eine recht nervige Angelegenheit, außer man willigt pauschal in alle Cookies ein. Das heißt aber auch, dass man dem Website-Betreiber jede Menge Daten zur Verfügung stellt. Wie transparent sind wir also? Und welche Informationen werden über uns gesammelt?

Hans-Dieter Neumann von der Deutschen Vereinigung für Datenschutz e.V. erklärt uns in diesem Podcast, was es mit den Cookies auf sich hat.

Zahorsky: Hallo Herr Neumann! Die Deutsche Vereinigung für Datenschutz, kurz DVD, ist eine unabhängige Bürgerrechtsvereinigung, die sich für Datenschutzbelange in Deutschland und Europa einsetzt. Im Zusammenhang mit Cookies ist das Thema Datenschutz wichtig. Vielleicht können Sie erstmal kurz erklären, was Cookies sind?

Neumann: Hallo Frau Zahorsky, zunächst einmal vielen Dank für die Einladung und die Möglichkeit, hier unser Anliegen vortragen zu dürfen.

Cookies sind Datensätze.[2] Sie werden beim Besuch einer Website auf dem Endgerät (Rechner, Tablet, Handy) gespeichert, u. a. um den Besucher wiederzuerkennen. Gespeichert werden diese Informationen vom Browser, den ein Nutzer verwendet. Leider ist immer noch zu oft die Aussage „Cookies sind kleine Textdateien" in den Datenschutzerklärungen vieler Websitebetreiber zu finden. Das mag früher einmal richtig gewesen sein - heute sind die Begriffe „klein" und „Text" verfehlt.

Die Speicherung von Cookies ist sicherlich sinnvoll, wenn es um die Erfassung von Anmeldedaten oder Spracheinstellungen geht. Diese Cookies, die technisch erforderlich sind, werden auch First-Party-Cookies genannt. Das gilt zum Beispiel auch für Cookies, die Websitebetreiber speichern, um den Betrieb sicherzustellen oder um Attacken nachverfolgen zu können.

Anders sieht das bei Third-Party-Cookies aus. Hier kommen Drittanbieter ins Spiel, über deren Aktivitäten die User informiert werden müssen. Diese Drittanbieter verfolgen eigene Interessen und wollen zum Beispiel Werbung bei dem User platzieren.

Mit Cookies – und auch anderen Tools – können Nutzer getrackt werden.[3] Tracking nenne ich auch ganz gerne datenanalytisches Stalking. Manchmal findet man anstelle von Tracking auch die Begriffe Customer Journey, Targeting, Retargeting oder auch Web-Analyse.

Zahorsky: Einer YouGov-Umfrage vom Mai 2020 zufolge lesen sich gut 40 Prozent der Befragten die Hinweise eh nicht durch, sondern klicken einfach auf „Okay" oder „Cookies akzeptieren". 12 Prozent verlassen die Seite direkt wieder. Warum ist der Cookie-Consent so kompliziert gestaltet? Für den User ist das doch sehr nervig.

Neumann: Ja Frau Zahorsky, da haben Sie ein wirklich gutes Beispiel erwischt, wie man aus einer guten Sache eine schlechte machen kann. Der EuGH hat am 01.10.2019 in einem Urteil[4] festgelegt, dass Tracking-Cookies, also Tools, die ein Individuum „aufspüren" können, nur dann verwendet werden dürfen, wenn dazu eine freiwillige, informierte und aktive Einwilligung vorliegt. Bei Gesundheitsdaten z. B. muss sie zudem in schriftlicher Form vorliegen. Eine Einwilligung ist eine von den drei Rechtsgrundlagen des Art. 6 DSGVO, die bei diesem Thema zur Anwendung kommen können. Sollte jedoch ein Vertrag geschlossen werden, dann ist das nicht erforderlich und auch nicht, wenn ein berechtigtes Interesse vorliegt. Das sind die beiden anderen gängigen Rechtsgrundlagen.

Diese Einwilligungen müssen über ein Consent-Banner eingeholt werden, bevor eine Website besucht werden kann. Ich sage deshalb nicht Cookie-Banner, weil nicht nur Cookies als Tracking Instrumente eingesetzt werden. Jetzt könnte man diese Banner schlicht gestalten und einen Button für eine Bestätigung und einen für eine Ablehnung bereit halten. Doch letzterer wird in der Regel durch einen Button „Einstellungen" ersetzt. Dort wird eine Liste mit Cookies aufgeführt, die gesetzeskonform deaktiviert sind.

Unter „Einstellungen" oder „Informationen" ist aber auch ein Button mit der Aufschrift „berechtige Interessen" zu finden. Und dort wiederum sind mehr

oder weniger lange Listen von Cookies aufgeführt, die bereits aktiviert sind und für eine Ablehnung deaktiviert werden müssen - manchmal einzeln, manchmal als Gesamtpaket. Und einige Websites bieten trotz Ablehnungen keine Speichermöglichkeit, sondern man muss alle Cookies dann doch noch akzeptieren, wenn man die Websites besuchen will. Es ist also nicht der Datenschutz, der das Leben schwierig macht, sondern oft genug dessen technische Umsetzung.

Zahorsky: Und was hat es mit der Entscheidung der belgischen Datenschutzbehörde APD auf sich, die besagt, dass ein zentraler Mechanismus für Cookie-Banner gegen die europäische Datenschutz-Grundverordnung DSGVO verstößt?

Neumann: Die belgische Datenschutzaufsicht hat gleich mehrere Punkte kritisiert. Der Verband für digitales Marketing und Werbung IAB Europe hat ein Instrument für das Einholen von Einwilligungen entwickelt, das Transparency & Consent Framework (TCF). Dieses vielgenutzte Tool wurde am 02.02.2022 von den Belgiern als datenschutzwidrig eingestuft und mit einem Bußgeld in Höhe von 250.000 Euro belegt.

Gründe dafür waren unter anderem die fehlende Rechtsgrundlage für die Einwilligungen, fehlende transparente Informationen zur Verarbeitung und die mangelnden Möglichkeiten zur Wahrnehmung von Betroffenenrechten. Zudem meint die Datenschutzaufsicht, dass IAB Europe auch für die Verarbeitung mitverantwortlich ist und keinen Datenschutzbeauftragten benannt hat.

Zahorsky: Mal angenommen, man willigt in alle Cookies ein: Welche Daten sammeln die dann?

Neumann: Oh je, dem Sammeltrieb sind praktisch keine Grenzen gesetzt. Von Interesse sind zum Beispiel Geräteinformationen wie Modell, Betriebssystem, Version, Browser oder Seriennummer bei Mobiltelefonen auch die IMEI, die eindeutige Gerätenummer. Neben Namen, persönlichen Daten und Standort sind auch Hobbys, Interessenlagen, Reisewünsche und -verhalten, Kaufobjekte, Preisniveaus, Zahlungsmodalitäten und viele andere Punkte von Interesse für die Werbeindustrie. Besonders interessant sind die Daten, wenn sie zu Profilen geformt werden können. Aber wer möchte schon, dass seine schlechten Blutdruckwerte aus der Health-App in der App seiner Krankenkasse gespeichert werden? In der Literatur[5] finden sich viele Beispiele, wo getrackte, aber auch frei abgegebene Informationen in Kombination mit anderen Informationsquellen zu Nachteilen von Betroffenen führen.

Zahorsky: Ziel der Datensammelei ist ja dann die personalisierte Werbung. Können Sie kurz erklären, wie das funktioniert?

Neumann: Hier können wir wieder auf das TCF von IAB Europe zurückkommen. In dem Augenblick, in dem User vor dem Besuch einer Website den Consent-Banner positiv bestätigen, wird ein Datenprofil des Nutzers an eine große Anzahl Unternehmen gesendet. Die Kriterien wie Kaufkraft und andere werden in Profilen zusammengestellt, nach denen Zielgruppen für Werbeanzeigen gebildet werden. Das Ganze geschieht in Bruchteilen von Sekunden. Werbetreibende blenden dann Anzeigen in die Apps oder in die Seiten der Suchmaschinen ein. Diese Anzeigen sollen dann – so der Anspruch des TCF – ganz auf die Bedürfnisse und Wünsche der User ausgerichtet sein.

Zahorsky: Abgesehen davon, dass die meisten User sich von Online-Werbung genervt fühlen: Was ist denn jetzt aber an personalisierter Werbung so schlecht? Werbung wird ja sowieso ausgespielt. Warum dann nicht eine, die mir unter Umständen ein für mich interessantes Produkt vorstellt?

Neumann: Ich möchte von Werbung nicht erschlagen werden, und die anderen User auch nicht. Natürlich ist es nicht schlecht, wenn ich zwei, drei Reisebüros anrufe und dort um Infos für mein Reiseziel bitte. Ich käme allerdings nicht auf die Idee in der Tageszeitung einen diesbezüglichen Aufruf zu starten. Ich will, dass nur ganz bestimmte, von mir ausgesuchte Anbieter meine Daten bekommen und letztendlich auch sichergehen, dass meine Daten nicht in falsche Hände geraten. Übrigens hat ein Kollege kürzlich sehr viel Werbung für ein Produkt erhalten, das er kurz zuvor gekauft hatte.

Zahorsky: Und wie kann man sich vor der Datenerhebung schützen? Welche Tipps haben Sie für unsere Hörer?

Neumann: Da gibt es eine Reihe von Maßnahmen, die man ergreifen kann, die aber dann auch ein wenig Arbeit verursachen können. An den Endgeräten, also am Rechner, Laptop oder Handy, können die User das Setzen der Cookies schon im Browser unterbinden. Die gängigen Browser bieten zudem Add-ons, also Browser-Erweiterungen, die das Tracken blockieren. Auch bei der Auswahl von Suchmaschinen sollte man schon Vorsicht walten lassen. Dann sollten alle Nutzer ihre Suchverläufe löschen, insbesondere dann, wenn das Endgerät auch von anderen Personen genutzt wird.

Auch sollte man sich überlegen, ob man nicht auf die heute etablierten und extrem aufmerksamkeitsheischenden Social-Media-Tools ganz verzichtet und zum Beispiel auf Mastodon oder andere Dienste aus dem Fediverse[6] zugreift. Nuudle[7] nur als Beispiel ist ein nicht-trackendes Termintool, mit dem man sehr bequem arbeiten kann.

Es gibt zudem viele hilfreiche Quellen, bei denen man wertvolle Tipps bekommt. Ich denke da an Digitalcourage[8], an den Blog von Mike Kuketz[9] oder auch an ethical.net[10], wo ein sehr üppiges Arsenal von Programmen, Apps und Diensten vorgestellt wird.

1 https://www.it-business.de/podcast/

2 https://dr-dsgvo.de/cookies-sind-keine-textdateien/

3 Benedikt, Kristin; Buckel, Alexander; Mammen, Jan-Hendrik: Web-Tracking nach DSGVO, 1. Aufl. 2019, Amazon (Selbstverlag), S. 11

4 https://curia.europa.eu/juris/document/document.jsf;jsessionid=D5DC4CA415C605B28E70747FD3C5158C?text=&docid=218462&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1&cid=1458627

5 Beispiel: Nocun, Katharina: Die Daten, die ich rief; Köln 2018

6 https://www.medienpaedagogik-praxis.de/2022/05/03/gelingt-mastodon-und-dem-fediverse-nun-der-durchbruch/

7 https://nuudel.digitalcourage.de/

8 https://digitalcourage.de/

9 https://www.kuketz-blog.de/

10 https://ethical.net/resources/

K.P. (Name der Redaktion bekannt)

Warum ich Facebook und Co. nutze …

Weil es heutzutage nicht ohne geht, wenn man am Ball bleiben will.

Ich gehöre zur älteren Generation und nutze Facebook und WhatsApp, allerdings durchaus unter kritischer Betrachtung. Mir ist immer bewusst, dass ich durch die Nutzung „ausspioniert“ werden kann. Markenartikler nutzen Social Media, um potenzielle Kunden mit Werbung zu versorgen.

Beispiel: Ich suche bei Google irgendein Produkt und ich kann sicher sein, dass ich die nächsten vier Wochen Werbung für dieses Produkt auf Facebook erhalte. Schlimmer noch, auch ähnliche Produkte, die vielleicht für mich von Interesse sein könnten, werden mir angezeigt. Das finde ich extrem nervig, aber ich nehme es in Kauf und mich beeinflusst das auch nicht in meinem Kaufverhalten.

Diese Werbeform wird heute von vielen Firmen genutzt, weil sie funktioniert. In keinem Medium kann man so zielgruppengenau werben, wie auf den Social-Media-Kanälen.

Dennoch ist es für mich inzwischen undenkbar ohne Facebook und Co. zu leben. Ich nutze die Plattform sehr gerne, um Leute ausfindig zu machen, ehemalige Schulfreunde z.B., oder um Erfahrungen in bestimmten Lebenssituationen in Interessensgruppen auszutauschen.

Politische Meinungen versuche ich auf Facebook nicht zu teilen, da mir dann oftmals der Umgang damit nicht gefällt. Leider gibt es heute ja Menschen, die in der Anonymität des Netztes der Meinung sind, sie können jeden Bullshit äußern. Da habe ich echte Probleme mit und möchte mich mit solchen Leuten nicht auseinandersetzen. Diskussionen in dieser Richtung führe ich nach wie vor lieber am Küchentisch oder in geselliger Runde in einer Kneipe.

Hier ist die Politik meiner Meinung nach gefordert Facebook und Co. dazu zu verpflichten, dass Hasskommentare sofort gelöscht werden und die Verfasser gesperrt werden. Aber soweit ich es mitbekommen habe, passiert da ja jetzt auch was.

WhatsApp nutze ich für die schnelle Kommunikation mit der Familie bzw. mit Freunden (Ich verspäte mich etc.). Möchte ich auch nicht mehr drauf verzichten, aber auch hier habe ich für mich Regeln aufgestellt, was den Umgang angeht.

Jeder, der im Internet unterwegs ist, muss sich darüber klar sein, dass seine Daten genutzt werden. Datenschutz ist sehr wichtig, aber ich habe es auch ein Stück weit selbst in der Hand, was ich von mir preisgebe. In diesem Bewusstsein macht es mir Spaß, auf Social-Media-Kanälen unterwegs zu sein.

Thilo Weichert

Betroffen von Datenschutzverstößen – Was tun?

Identitätsklau, Werbe-Cookies ohne Einwilligung, Abgreifen von Fotos im Internet, Diffamierung in sog. sozialen Netzwerken, Gesundheitsdaten in der Personalverwaltung, fremde Videoüberwachung im eigenen Garten … Werden derartige, oft im Verborgenen praktizierte Verstöße gegen den Datenschutz den Betroffenen bekannt, stellt sich für diese die Frage: „Was kann ich dagegen tun?“ Diese einfache Frage stößt auf eine komplexe Realität: Unklar ist oft, welche Technik genutzt wird, wer den Angriff veranlasst hat und wer dafür verantwortlich ist, wer hiergegen wirksam vorgehen könnte und tatsächlich kann, welche Möglichkeiten rechtlich und welche realistischerweise bestehen.

Vorneweg: Deutschland und die Mitgliedsstaaten der Europäischen Union (EU) sind demokratische Rechtsstaaten, die Grundrechte gewährleisten. Es gilt das in Art. 8 der europäischen Grundrechte-Charta garantierte Recht auf Datenschutz. Es gilt zudem die europäische Datenschutz-Grundverordnung (DSGVO), die eine Vielzahl von sog. Betroffenenrechten regelt: allen voran das Recht auf Auskunft (Art. 15 DSGVO), zudem ein Recht auf Löschung, sogar „auf Vergessenwerden“ (Art. 17 DSGVO), ein Recht auf Datenberichtigung (Art. 16 DSGVO), ein Recht auf Datensperrung oder wie es in Art. 18 DSGVO heißt: „auf Einschränkung der Verarbeitung“. Betroffene müssen über die sie betreffende Datenverarbeitung informiert werden (Art. 13, 14 DSGVO). Sie können mit persönlichen Gründen einer Datenverarbeitung widersprechen (Art. 21 DSGVO). Im Fall eines Verstoßes haben sie einen Anspruch auf Entschädigung, auf materiellen oder immateriellen Schadenersatz (Art. 82 DSGVO). Zivilrechtlich bestehen Ansprüche auf Unterlassung und Beseitigung von unzulässigen informationellen Angriffen (§ 823 i.V.m. § 1004 BGB analog). Und um das alles durchzusetzen, garantiert die DSGVO ein Recht auf Beschwerde bei einer Aufsichtsbehörde

(Art. 77), ein Recht auf wirksamen gerichtlichen Rechtsschutz gegen Verantwortliche oder Auftragsverarbeiter (Art. 79) und sogar ein Recht auf wirksamen gerichtlichen Rechtsbehelf gegen eine Aufsichtsbehörde (Art. 78).

Das hört sich alles gut an. In der Realität kann sich aber schnell Ernüchterung einstellen, wenn von den gesetzlichen Versprechungen in Wirklichkeit wenig und manchmal gar nichts übrig bleibt. Dass Gesetze nicht zu 100 Prozent durchgesetzt werden, ist in einem freiheitlichen Staat normal: Es gibt nicht nur gesetzestreue Bürgerinnen und Bürger und erst recht nicht nur gesetzestreue Unternehmen. Und die totale Durchsetzung von Gesetzen würde eine Totalkontrolle nötig machen. Deshalb sind Abstriche bei den Erwartungen an die gesetzliche Ordnung zu machen. Dabei wäre es aber wünschenswert, dass schwere Verletzung eher schneller und nachhaltiger verfolgt und sanktioniert werden als unbedeutende Datenschutzverstöße.

Doch auch das ist nicht Realität: Es ist oft gerade umgekehrt. Einige Gründe dafür liegen auf der Hand: Die zuständigen Aufsichtsbehörden sind zu schlecht ausgestattet und haben zu viel zu tun. Das Bewusstsein über die Notwendigkeiten beim Datenschutz fehlt bei Vielen. Und dann gibt es viele Menschen, die vom Datenschutz nichts halten und sich deshalb auch nicht veranlasst sehen sich an die Gesetze zu halten. Es gibt noch einen weiteren Grund für die Vollzugsdefizite beim Datenschutz: Für viele Unternehmen ist es profitabel unter Missachtung des Datenschutzes ihre Geschäfte zu machen; ihr Geschäftsmodell beruht darauf, dass sie unter Verletzung von Gesetzen Daten sammeln und nutzen und dabei gewaltige Profite machen, während die Gefahr, dafür sanktioniert zu werden, immer noch gering ist.

Umso wichtiger ist es, dass Betroffene darauf Einfluss nehmen können, dass ihre Datenschutzrechte beachtet werden. Im Folgenden werden die Möglichkeiten dargestellt und welche Erfolgschancen damit einhergehen. Anspruch und Wirklichkeit sind auch bei der Wahrnehmung der Betroffenenrechte nicht identisch. Konkret geht es um folgende Mechanismen:

1. Wahrnehmung der eigenen Rechte direkt gegenüber dem Verantwortlichen und dessen Datenschutzbeauftragten
2. Beschwerde bei den Datenschutzaufsichtsbehörden
3. Einschaltung von Verbraucherzentralen
4. Gang in die Öffentlichkeit.

Bei allen o.g. Aktivitäten muss der Betroffene nicht persönlich tätig werden, sondern kann sich durch eine andere Person vertreten lassen. Wenn hierbei Rechtswirkungen ausgelöst werden sollen, ist es im Fall der Vertretung, z.B. durch einen Anwalt, nötig, dass im Zweifelsfall eine wirksame Vertretungsvollmacht vorgelegt wird.

1. Geltendmachung der Betroffenenrechte beim Verantwortlichen

Es ist sinnvoll, bevor weitere Schritte eingeleitet werden, sich zunächst an die die Daten verarbeitende, also die verantwortliche Stelle zu wenden. Das ist die, welche die Daten erhebt und weiterverarbeitet, also z.B. das Handelsunternehmen, der Webseitenbetreiber, der Arbeitgeber oder die Behörde. Oder es handelt sich um einen Auftragsverarbeiter, der für einen Verantwortlichen tätig wird. Um die korrekte Adresse herauszubekommen, gibt es im Internet die Impressumspflicht (§§ 5, 6 Telemediengesetz – TMG). Dort müssen auf der Startseite im Web – oder zumindest mit einem weiteren Klick erreichbar – der Name, die Adresse und eine elektronische Kontaktangabe aufgeführt werden. Zumeist unter der Rubrik „Datenschutz“ (und dort leider zumeist erst ganz am Ende) finden sich Kontaktangaben zum betrieblichen Datenschutzbeauftragten, die der Verantwortliche nach Art. 37 Abs. 7 DSGVO zu veröffentlichen verpflichtet ist. Art. 38 Abs. 4 DSGVO regelt, dass Betroffene sich zur Wahrnehmung ihrer Rechte an den Datenschutzbeauftragten wenden können. Es gibt interne wie externe Datenschutzbeauftragte, also solche in der Stelle selbst, und solche, die selbstständig tätig sind, etwa Rechtsanwälte, spezialisierte Datenschutzfachleute oder -firmen.

Man muss sich als Betroffener mit einer Beschwerde nicht an den Datenschutzbeauftragten wenden; Adressat kann auch die Stelle generell oder und deren Leitung sein. Ist dort nicht bekannt, wie mit einer Datenschutzanfrage umzugehen ist; dann liegt es nahe den insofern ausgebildeten Datenschutzbeauftragten einzuschalten.

Ist unklar, welche Daten bei der Stelle für welche Zwecke und auf Grund welcher Rechtsgrundlage verarbeitet werden, woher die Daten stammen und an wen sie weitergegeben werden, dann empfiehlt sich die Inanspruchnahme des Auskunftsrechts gegenüber der Stelle (Art. 15 DSGVO). Eine Begründung hierfür ist nicht nötig. Um Ausflüchte der Stelle zu vermeiden, ist es sinnvoll den Anlass des Auskunftsersuchens darzustellen. Hat der Verantwortliche Zweifel an der Identität des Betroffenen, so kann er deren Glaubhaftmachung einfordern. Ein bestimmtes Verfahren, z.B. durch Vorlage eines Personalausweises oder Übersendung einer Kopie, kann dabei nicht vorgegeben werden, doch sollte man sich an entsprechendes Vorschlägen orientieren.

Das Ersuchen kann analog oder digital erfolgen und sollte eine Fristsetzung enthalten (z.B. zwei Wochen). Nach erfolglosem Ablauf der Frist sollte zeitnah die Auskunftserteilung angemahnt werden. Erfahrungsgemäß sind erste Antworten hinhaltend („Bitte um etwas Geduld“) oder ausweichend (z.B. „alle Daten, die im Rahmen des Vertragsverhältnisses nötig sind“ oder „alle Daten, die Sie angegeben haben“). Solche Antworten sind ungenügend. Es muss auf Nachfrage präzise angegeben werden, welche konkreten Daten vorliegen und verarbeitet werden. Bleibt die Auskunft aus oder ist sie unzulänglich, so ist das ein Verstoß gegen Art. 15 DSGVO, der von der Aufsichtsbehörde sanktioniert werden kann.

Analog zum Vorgehen zwecks Erlangung einer Auskunft kann bei der Umsetzung der anderen Betroffenenrechte (Löschung, Berichtigung, Verarbeitungsbeschränkung, Widerspruch, Schadenersatz, Unterlassung, Beseitigung) vorgegegangen werden.

Die Erfahrung lehrt, dass Verantwortliche auf eine Betroffenenanfrage oder -beschwerde zunächst nicht adäquat und rechtskonform antworten, jedenfalls dann nicht, wenn sie z.B. einen

Rechtsverstoß verbergen wollen. In solchen Fällen ist es sinnvoll mit Fristsetzung nochmals nachzuhaken, bevor andere und weitere Schritte eingeleitet werden. Alle weiteren Maßnahmen sind aufwändiger, schwerfälliger und zeitintensiver.

Statt den weiter unten noch beschriebenen Vorgehensweisen besteht bei einer unbefriedigenden (rechtswidrigen) Reaktion oder einer Nichtreaktion der angeschriebenen Stelle die Möglichkeit gegen den Verantwortlichen direkt Klage zu erheben. Bei Klagen gegen Privatunternehmen ist der Zivilrechtsweg gegeben, Klagen gegen öffentliche Stellen, also gegen Behörden, werden vor dem Verwaltungsgericht verhandelt (Art. 79 DSGVO).

2. Beschwerde bei der Aufsichtsbehörde

Gemäß Art. 77 Abs. 1 DSGVO haben Betroffene „unbeschadet eines anderweitigen ... gerichtlichen Rechtsbehelfs das Recht auf Beschwerde bei einer Aufsichtsbehörde, insbesondere in dem Mitgliedstaat ihres gewöhnlichen Aufenthaltsorts, ihres Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes“. Ist man von einem Verstoß nicht persönlich betroffen, kann dennoch eine Beschwerde eingereicht werden. Es liegt dann aber im freien Ermessen der Datenschutzaufsichtsbehörde, ob sie tätig wird oder nicht. Es ist – angesichts der hohen Arbeitslast, die bei den meisten Aufsichtsbehörden besteht – eher ungewöhnlich, dass eine Aufsichtsbehörde auf eine Beschwerde von Nichtbetroffenen mit Ermittlungen reagiert. Etwas anderes gilt, wenn zum gleichen Thema viele Beschwerden vorliegen oder es sich nach ihrer Ansicht um einen so schwerwiegenden Vorwurf handelt, dass sie von Amts wegen tätig wird.

Aus Art. 77 Abs. 1 DSGVO geht hervor, dass die Beschwerde bei der Behörde des Wohnsitzes, des Arbeitsplatzes oder der tatsächlichen Datenverarbeitung eingereicht werden kann. Diese Behörde ist dann auch für die Zwischen- und die Endnachricht zuständig (Art. 77 Abs. 2 DSGVO). Bearbeitet wird die Beschwerde aber regelmäßig ausschließlich durch die sog. „federführende Aufsichtsbehörde“, die für die europäische Hauptniederlassung des Unternehmens (vgl. Art. 4 Nr. 16 DSGVO) des Verantwortlichen zuständig ist (Art. 60 DSGVO). Diese federführende Behörde leitet die Ermittlungen und kann sich dabei von anderen Aufsichtsbehörden unterstützen lassen (Art. 61 DSGVO). In jedem Fall muss sie alle „betroffenen Aufsichtsbehörden“ einbeziehen. Dies sind die Aufsichtsbehörden, in deren Gebiet eine Niederlassung des Verantwortlichen besteht oder sich erhebliche Auswirkungen der Verarbeitung zeigen, sowie die, bei denen eine Beschwerde eingereicht wurde (Art. 4 Nr. 22 DSGVO). Die federführende und alle anderen betroffenen Aufsichtsbehörden versuchen eine einheitliche Entscheidung zu treffen (Art. 62 DSGVO); wenn dies misslingt, wird im Rahmen eines komplizierten Verfahrens eine Mehrheitsentscheidung gesucht (Art. 63 ff. DSGVO).

Der Betroffene hat also die Möglichkeit bei seiner Beschwerde zwischen verschiedenen Aufsichtsbehörden zu wählen. Wenn er die Sprache der federführenden Aufsichtsbehörde im Ausland beherrscht, ist es sinnvoll die Beschwerde direkt dort einzureichen. Ansonsten ist es naheliegend die Behörde am Wohnort oder am Arbeitsplatz zu befassen. Da die Kommunikation zwischen den Aufsichtsbehörden zumeist in Englisch erfolgt, ist es auch möglich in dieser Sprache die Beschwerde einzureichen; dies ist bei internationalen Vorgängen bei jeder Aufsichtsbehörde möglich.

Strategische Erwägungen können es sinnvoll erscheinen lassen zu einem Sachverhalt bei verschiedenen Aufsichtsbehörden Beschwerden zu erheben, insbesondere wenn der federführenden Behörde wenig vertraut wird (was bisher mit berechtigten Gründen immer wieder bei der irischen Aufsicht der Fall ist, die europaweit für viele internationale IT-Konzerne federführend ist, weil deren europäischer Hauptsitz in Irland liegt, siehe auch S. 93). Dadurch sind alle Beschwerdeadressaten „betroffene Aufsichtsbehörden“ und haben ein Mitentscheidungsrecht bei der abschließenden Entscheidung. Insbesondere bei internationalen NGO-Kampagnen wird immer gerne zu dem Mittel gegriffen möglichst viele Behörden einzubeziehen. Dies erhöht den Entscheidungsdruck: damit geht aber auch eine gewisse Verkomplizierung und Verlangsamung des Gesamtverfahrens einher.

In der Regel besteht in jedem EU-Mitgliedsland eine Aufsichtsbehörde. Rechtlich angegliedert an das EU-Verfahren nach der DSGVO sind einige wenige weitere Staaten im Europäischen Wirtschaftsraum (EWR): Norwegen, Island und Liechtenstein. Die Adressen der europäischen Aufsichtsbehörden finden sich im Internet unter

https://www.bfdi.bund.de/DE/Service/Anschriften/Europa/Europa-node.html.

Für Stellen der Europäischen Union (EU) ist der Europäische Datenschutzbeauftragte zuständig:

https://edps.europa.eu/_de.

Das einzige EU-Mitgliedsland mit einer föderalen Struktur bei der Datenschutzaufsicht ist Deutschland. Hier gilt insofern das Bundesdatenschutzgesetz (BDSG). Für öffentliche Stellen des Bundes ist der Bundesbeauftragte für den Datenschutz zuständig (§ 9 Abs. 1 BDSG), ebenso für die Telekommunikations- und Postunternehmen (§ 29 Abs. 1 TTDSG, § 42 Abs. 3 PostG) sowie in einigen sozialrechtlich dominierten Spezialbereichen (z.B. Jobcenter, § 50 Abs. 2 SGB II, länderübergreifende Gesundheitsforschung, § 287a SGB V). Die Landesbeauftragten für den Datenschutz sind für die öffentlichen Stellen in den Ländern zuständig sowie für die nicht-öffentlichen Unternehmen mit dem Hauptsitz in den jeweiligen Bundesländern (§ 40 Abs. 1 BDSG). In Bayern sind für den öffentlichen und den nicht-öffentlichen Bereich unterschiedliche Aufsichtsbehörden zuständig.

Die Adressen der Aufsichtsbehörden in Deutschland finden sich im Internet unter

https://www.bfdi.bund.de/DE/Service/Anschriften/Laender/Laender-node.html.

Weiter wird die Aufsichtsstruktur in Deutschland dadurch verkompliziert, dass es für die Gerichte sowie für die Kirchen und die Rundfunkanstalten eigenständige Aufsichtszuständigkeiten gibt:

https://www.bfdi.bund.de/DE/Service/Anschriften/Kirchen/Kirchen-node.html und

https://www.bfdi.bund.de/DE/Service/Anschriften/Rundfunk/Rundfunk-node.html.

Formale und inhaltliche Voraussetzungen für Datenschutzbeschwerden

gibt es nicht. Doch sollten einige Aspekte beachtet werden: Unabdingbar ist es, wenn man auf eine Beschwerde hin auch eine Antwort bzw. Reaktion erwartet, dass die eigenen Erreichbarkeitsdaten präzise benannt werden, also Name, Adresse, möglichst Telefonnummer und E-Mail-Adresse. Fehlt es an den beiden letztgenannten Angaben, werden Rückfragen der Datenschutzaufsicht erschwert. Auf welche Art die Beschwerde die Aufsicht erreicht, ist unwichtig: Post, Fax, Internetformular, Mail, ja theoretisch sind sogar Telefon, persönliche Beschwerde vor Ort oder SMS möglich.

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) stellt im Internet ein Beschwerdeformular zur Verfügung:

https://formulare.bfdi.bund.de

Entsprechendes gilt für fast alle anderen Aufsichtsbehörden.

Es ist sinnvoll den Beschwerdegrund so präzise wie möglich zu benennen. Alles, was zur Aufklärung einer vermeintlich unzulässigen Datenverarbeitung bekannt ist, sollte gleich beim ersten Anschreiben benannt werden: Name, Adresse, Standortangaben des Verantwortlichen oder Auftragsverarbeiters sind wichtig, um die Zuständigkeit festzustellen. Weiterhin ist es angebracht präzise Angaben zum Beschwerdegrund zu machen: Angaben zu Ort und Zeit, Umstände und – wenn bekannt – über technische Details. Eine juristische Einordnung ist nicht nötig, aber auch nicht schädlich; sie erleichtert dem Sachbearbeiter die erste Einordnung. Dieser hat aber insofern – davon sollte man ausgehen – die nötige Sachkompetenz. Abschließend sollte mitgeteilt werden, was angestrebt wird, z.B. eine Auskunftserteilung, eine Datenlöschung oder eine Sanktionierung.

Das Beschwerdeverfahren bei der Datenschutzaufsicht ist für die Betroffenen kostenfrei.

Für die weitere Bearbeitung sollte die Datenschutzaufsicht wissen, ob gegenüber dem vermeintlichen Verletzer des Datenschutzes der Name der Beschwerde führenden Person bzw. des Betroffenen genannt werden kann. Geht es um einen individuellen Datenschutzverstoß, so geht hieran regelmäßig kein Weg vorbei. Handelt es sich dagegen um systematische und strukturelle Verletzungen des Datenschutzes, ist die Identität der Beschwerdeperson nicht von Bedeutung. Es besteht dann die Möglichkeit und bei Wunsch der Anspruch gegenüber dem Verletzer anonym zu bleiben. Das kann sogar wichtig sein, wenn es sich bei dem Verantwortlichen z.B. um den eigenen Arbeitgeber handelt und man von diesem Ärger befürchtet, wenn der von dem Urheber der Datenschutzbeschwerde erfährt. Aber auch bei einem Arzt oder Krankenhaus kann die Befürchtung bestehen nicht mehr oder nicht so gut behandelt zu werden oder bei einem Handelsgeschäft nicht mehr bedient oder beliefert zu werden. Besteht man als Beschwerdeführer auf einer anonymen Bearbeitung, so darf die Aufsicht gegenüber dem Verantwortlichen die Identität des Beschwerdeführers nicht offenlegen.

Auf eine Beschwerde hin erhält man regelmäßig zunächst eine Eingangsbestätigung mit einem Aktenzeichen und evtl. weitere Informationen zum Fortgang der Untersuchung. Diese Untersuchung beschränkt sich oft darauf, dass die Stelle, gegen die sich die Beschwerde richtet, um eine Stellungnahme gebeten wird. Die Erwartung, dass die Behörde unangekündigt vor Ort eine Prüfung vornimmt, ist zumeist unrealistisch. Derartiges ist aber rechtlich möglich und geschieht in Ausnahmefällen, etwa wenn es sich um einen gravierenden und systematischen Verstoß handeln könnte, den die Stelle – z.B. durch eine Datenlöschung – evtl. zu vertuschen versucht. Der ersten Stellungnahme folgt zumeist ein weiterer Austausch zwischen verarbeitender Stelle und Datenschutzaufsicht, regelmäßig unter Einbeziehung des Datenschutzbeauftragten der Stelle, evtl. auch der IT-Administration, der Stellenleitung oder einer anwaltlichen Vertretung der Stelle. Dieser Austausch – der nicht selten ein unergiebiges Ping-Pong ist, bei dem die Stelle abwiegelt, lügt oder gar zum Gegenangriff geht – verliert sich in einigen Fällen im Nirgendwo.

Immer wieder bleibt es dann für den Beschwerdeführer bei der Eingangsbestätigung: Die Aufsichtsbehörden arbeiten oft am Limit und sind oft mit den verfügbaren Kapazitäten nicht in der Lage allen Beschwerden nachzugehen. Es ist leider auch nicht selten, dass man einen abwiegelnden Bescheid erhält, der der möglicherweise falschen Darstellung des vermeintlichen Verletzers ohne Weiteres Glauben schenkt. In solchen Fällen geht kein Weg daran vorbei falsche Behauptungen richtig zu stellen und – wenn möglich – mit Beweisen zu bekräftigen.

Wird von der Aufsicht ein Datenschutzverstoß festgestellt, so sollte auch eine Sanktion erfolgen. Die möglichen Sanktionen sind in Art. 58 Abs. 2 und Art. 83 DSGVO beschrieben. Sie beginnen mit einer Verwarnung und gehen bis zur Untersagung des Systembetriebs oder bis zu einem Bußgeld in Höhe von 4% des weltweiten Jahresumsatzes eines Unternehmens (Art. 83 Abs. 4, 5 DSGVO). Möglich ist zudem ein Strafantrag (§ 42 Abs. 2 BDSG). Die Herrschaft über ein auf einen Strafantrag oder eine Strafanzeige ausgelöstes Ermittlungsverfahren liegt nicht mehr bei der Datenschutzaufsicht, die dann nur noch zuliefert, sondern bei der Staatsanwaltschaft. Es ist auch möglich, dass die Öffentlichkeit, z.B. über eine Presseerklärung der Aufsichtsbehörde über einen Verstoß informiert wird.

Im Fall von berechtigten Beschwerden kann eine Bearbeitung lange, ja Jahre, dauern. Ob es zu einer Sanktion kommt, hängt von vielen Aspekten ab: Der Verstoß muss lückenlos nachgewiesen werden können. Anwaltlich vertretene Stellen wehren sich zumeist mit allen rechtlichen Mitteln gegen Sanktionen. Manche Aufsichtsbehörde scheut – schon wegen des Aufwands – die gerichtliche Auseinandersetzung mit dem Datenschutzverletzer.

Der Beschwerdeführer sollte jeweils über den Stand des Verfahrens und letztlich über das Ergebnis der Beschwerde einschließlich der Möglichkeit eines gerichtlichen Rechtsbehelfs informiert werden (Art. 77 Abs. 2 DSGVO).

Der Betroffene kann gegen ihn betreffende (Abschluss-)Entscheidungen der Aufsichtsbehörde gerichtlich vorgehen (Art. 78 DSGVO). Mit einer Untätigkeitsklage kann allenfalls erreicht werden, dass eine eingeschlafene Ermittlung wieder lebendig gemacht wird. Eine Klage gegen einen ablehnenden Bescheid

der Aufsicht kann dagegen äußerst effektiv sein. Dabei wird nicht nur die Richtigkeit der Verwaltungsentscheidung überprüft, sondern – inzident – ob ein Datenschutzverstoß vorlag. Da dies die verarbeitende Stelle betrifft, wird diese regelmäßig in solchen Verfahren beigeladen, so dass das Verfahren vor dem Verwaltungsgericht zugleich auch Wirkung gegenüber dem möglichen Datenschutzverletzer hat.

3. Einschaltung des Verbraucherschutzes

Schon seit vielen Jahren besteht die Möglichkeit sich mit einem Datenschutzanliegen auch an eine Verbraucherschutzorganisation, also z.B. eine Verbraucherzentrale, zu wenden und sich dort beraten und evtl. gar vertreten zu lassen. Zunächst stand dabei die Nutzung rechtswidriger allgemeiner Geschäftsbedingungen (AGB) zur Datenverarbeitung im Vordergrund (§§ 305 ff BGB). Seit 2016 wurde eine Regelung im Unterlassungsklagegesetz (§ 2 Abs. 2 Nr. 11 UKlaG) eingeführt, wonach Verbraucherorganisationen im Wege der Unterlassungsklage gegen materiell-rechtliche Datenschutzverstöße vorgehen können. Hiervon machen regionale Verbraucherzentralen und bundesweit vor allem der Verbraucherzentrale Bundesverband e.V. (vzbv = der Zusammenschluss der Verbraucherorganisationen) zunehmend Gebrauch. Hierbei geht es dann regelmäßig um schwerwiegende systematische Verstöße von großen Unternehmen mit einer großen Streubreite, insbesondere im Bereich der Internet-Wirtschaft.

Diese Klagemöglichkeit in Form der Verbandsklage ist in Art. 80 Abs. 2 DSGVO ausdrücklich vorgesehen. Solche prominenten Klagen landen immer wieder beim Europäischem Gerichtshof (EuGH), der dann europaweit geltende Grundsatzentscheidungen fällt.

Die Verbraucherzentralen sind aber auch eine geeignete Anlaufstelle für Betroffene zwecks Beratung bei vermuteten Datenschutzverstößen. Sie geben Hinweise, wie man selbst seine Rechte wahrnehmen kann, unterstützen hierbei oder verweisen auf die Beschwerdemöglichkeit bei den Datenschutzaufsichtsbehörden. Die Aufsichtsbehörden arbeiten teilweise mit den regionalen, den nationalen und den europäischen Verbraucherorganisationen zusammen. Bei Klagen nach dem UKlaG werden die Aufsichtsbehörden oft mit eingebunden (§ 12a UKlaG).

Seit 2018 ist es für Verbraucherschutzorganisationen auch möglich, für eine Vielzahl von Verletzten von Datenschutzverstößen gemäß dem Musterfeststellungsklagegesetz eine gerichtliche Vorklärung von Betroffenenansprüchen durchführen zu lassen. In Art. 80 Abs. 1 DSGVO ist sogar vorgesehen, dass Verbraucherschutzorganisationen umfassend für Geschädigte von Datenschutzverstößen, etwa zwecks Erstreitung von Schadenersatzansprüchen, gerichtlich vorgehen können. Die dafür nötige spezifische gesetzliche Grundlage besteht aber in Deutschland noch nicht; in der EU bereitet man derzeit gerade eine solche Grundlage vor (DANA 1/2021, 51 f.).

4. Gang in die Öffentlichkeit

Die schnellste Reaktion auf einen Datenschutzverstoß kann darin bestehen hierüber die Öffentlichkeit zu informieren. Damit wird der Verstoß zwar nicht abgestellt, doch kann so evtl. ein gewisser Druck auf den Datenschutzverletzer ausgeübt werden. Zudem besteht die Möglichkeit andere Betroffene zu informieren und zu mobilisieren. Einen Effekt hat dieser Gang in die Öffentlichkeit aber nur, wenn dadurch die Öffentlichkeit auch erreicht wird. Voraussetzung ist dafür, dass der Verstoß eine besondere Schwere hat und Dritte anspricht. Weitere Voraussetzung ist es, dass die Vorwürfe gut begründet sind und erläutert werden. Bei falschen Darstellungen läuft man Gefahr von der angegriffenen Stelle kostenpflichtig abgemahnt zu werden. Anwälte von angegriffenen Firmen haben erfahrungsgemäß keine Skrupel, wenn sie meinen, dass das von ihnen vertretene Unternehmen unberechtigterweise angegriffen wird oder wenn sie glauben mit einer Unterlassungserklärung Kritiker zum Schweigen bringen zu können.

Um sich rückzuversichern, ist evtl. die Einbindung von Nichtregierungsorganisationen (NGOs) sinnvoll. Doch auch diese werden einen Datenschutzverstoß nur dann aufgreifen, wenn er eine grundsätzliche oder größere Bedeutung hat. Die NGOs können ihre Veröffentlichungskanäle nutzen, um vor allem ihre Anhänger und auch die Presse zu erreichen.

Eine solche NGO ist z.B. der Digitalcourage e.V., der jährlich schlimme Datenkraken mit dem BigBrotherAward negativ auszeichnet. Bei vor allem technisch bedingten Datenschutzverstößen kann es sinnvoll sein, sich an den Chaos Computer Club (CCC) zu wenden. Bei Verstößen durch öffentliche Stellen, also Behörden wie insbesondere Polizei und Nachrichtendienste, engagiert sich die Gesellschaft für Freiheitsrechte e.V. (GFF) für die Beachtung des Datenschutzrechts und organisiert bzw. unterstützt musterhafte Klagen vor Gericht. Unterstützung ist auch durch die Deutsche Vereinigung für Datenschutz e.V. (DVD) möglich. Über den deutschsprachigen Bereich hinausgehend engagiert sich noyb (non of your business) mit Sitz in Wien für den Datenschutz. noyb versucht auch durch gerichtliche Musterklagen gegen Datenkraken vorzugehen.

Eine besondere Art des Widerstands gegen systematische Datenschutzverstöße sind über das Internet organisierte Kampagnen. Doch hier sollte man – wie bei allen im Internet durchgeführten Aktionen – darauf achten, dass man sich nicht vor einen falschen Karren spannen lässt: So manche Online-Kampagne nutzt die Empörung über (vermeintliche) Datenschutzverstöße, um ganz andere Ziele als den digitalen Grundrechtsschutz zu verfolgen.

Schlussbemerkungen

Die Vollzugsdefizite beim Datenschutz sind gewaltig. Dies ist so, seit es Datenschutz gibt. Mit der DSGVO besteht seit 2018 ein rechtlicher Rahmen, mit dem man sich wirksamer zur Wehr setzen kann. Doch für den „Normalbürger" bleibt der Weg zur Verteidigung seines „Rechts auf informationelle Selbstbestimmung" schwierig, zumal es sich zumeist um komplexe technische Vorgänge handelt und die Rechtslage unübersichtlich ist. Dann sind Betroffene auf externe qualifizierte oder gar professionelle Hilfe angewiesen. Hierfür

gibt es gemäß der DSGVO vorrangig die unabhängigen Datenschutzaufsichtsbehörden. Diese können aber auch nur einen bedingten Schutz gewährleisten, weshalb weitere Instanzen zur Wahrung des Datenschutzes in Betracht kommen: Verbraucherschützer, Nichtregierungsorganisationen, die Medien. Letztlich geht es nicht nur um den individuellen Datenschutz, sondern darum, dass wir in einer freien, d.h. auch möglichst überwachungsfreien Gesellschaft leben, in der wir unsere Grundrechte und Freiheiten selbstbestimmt wahrnehmen können. Die gesellschaftliche Durchsetzung des Datenschutzes bleibt dabei davon abhängig, dass viele Einzelne ihre Rechte in Anspruch nehmen. Es handelt sich hier um einen dauernden, immer wieder neu zu führenden Kampf, weil für Staat und Wirtschaft informationelle Fremdbestimmung von Menschen immer wieder attraktiv erscheint.

Heinz Alenfelder

Mit der Gießkanne gegen Flächenbrände? – Tipps im Internet zur datenschutzgerechten Nutzung sozialer Medien


Bild: iStock.com/ Mr. Ilkin / Dimple Bhati

Eine aktuelle Studie[1] der australischen University of New South Wales stellt fest, dass Twitter-Nutzerinnen und -Nutzer während der Covid-19-Pandemie unbeabsichtigt mehr personenbeziehbare Informationen preisgaben als vor der Pandemie. Die über 10 Millionen untersuchten Tweets während der Lockdown-Phasen in Australien, Indien, Großbritannien und den Vereinigten Staaten beschäftigten sich im wesentlichen mit der Unterstützung der Wirtschaft und der aktuellen Politik. Die Untersuchung zeigte, dass das Risiko der Identifizierung durch Ortsangaben oder Offenbarung sozialer Umstände in den Tweets stark wuchs: Teils reichten nur drei einzelne Tweets aus, um zuvor anonymisierte User zu identifizieren.

Ungeachtet solcher Gefahren steigt weiterhin die Zahl der Posts auf den Plattformen der sozialen Netzwerke. Die Webseiten mit Empfehlungen zum Datenschutz bei sozialen Medien sind allerdings auch recht zahlreich vertreten. Dieser Beitrag soll einige dieser Ratgeberseiten inhaltlich umreißen, voneinander abgrenzen und eine erste Bewertung vornehmen. Die wichtigsten Empfehlungen werden abschließend zusammengefasst.

Allen voran gibt das BSI „leicht umsetzbare Tipps, mit denen Sie das sozia-

le Leben im Internet einfach aBSIchern [sic!] können“[2]. Erwähnt werden sichere Passwörter, Zwei-Faktor- Authentisierung und die Empfehlung nicht unüberlegt auf Links oder Buttons zu klicken. Dann folgen weitere Infos zum Umgang mit dem Mobilgerät (Vorsicht bei App-Installation, Sperre des Geräts). Bezüglich eines Identitätsdiebstahls wird vor unüberlegten Kontaktanfrage-Bestätigungen gewarnt und der Privatsphäre-Schutz allgemein angesprochen. Besonders fällt auf, dass das BSI beim Löschen des Accounts darauf hinweist zunächst „bei Bedarf […] Daten außerhalb des Netzwerkes“ zu sichern und dann erst im Account zu löschen. Abschließend wird auf eine Übersicht der technischen Einstellungen für die „beliebtesten Plattformen wie Facebook, WhatsApp, Instagram und Twitter“ verwiesen. An anderer Stelle[3], auf die auch die Webseite des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit verweist[4], sind drei Ratschläge nochmal einfacher aufbereitet: „Auf persönliche Informationen achten“, „Sichere Passwörter verwenden“ und „Zwei-Faktor-Authentisierung verwenden“. Warum dies als „Frühjahrsputz im Internet“ bezeichnet wird, erschließt sich leider nicht.

Im Virtuellen Datenschutzbüro wird das Thema nur kurz behandelt[5], indem auf die drohenden Gefahren hingewiesen wird. Es folgen keine weiteren konkreten Tipps und auch die Verweise auf Material bei einzelnen Datenschutzbeauftragten führen insofern nicht weiter, als sich dieses vor allem an Unternehmen und Behörden wendet. Allerdings finden sich auf den Seiten einzelner Landesdatenschutzbeauftragter durchaus konkrete Anregungen für Verbraucherinnen und Verbraucher. In Nordrhein-Westfalen[6] wird das Thema problematisiert und dann werden acht Tipps gegeben, unter ihnen das Melden von Auffälligkeiten an das soziale Netzwerk und der Hinweis den Browserinhalt zu löschen, wenn der Netzwerkzugang von einem fremden Rechner aus erfolgte. Am Schluss erfolgt dort ein Hinweis auf die Verbraucherzentralen, leider ohne konkrete Links. Und schon 2018 gab die Berliner Datenschutzbeauftragte Smoltczyk eine empfehlenswerte Broschüre „Ich suche dich. Wer bist du?“ mit Tipps für Jugendliche zum Datenschutz bei sozialen Netzwerken heraus[7]. Mit Skepsis ist dort lediglich das Schlussfazit zu betrachten: „Soziale Netzwerke sind eine tolle Kommunikationsform und wenn du unsere 10 Tipps beachtest, schützt du mit einfachen Mitteln deine Privatsphäre ohne auf die Vorteile zu verzichten“.

Der 2006 gegründete Verein „Deutschland sicher im Netz (DsiN)“, in dem große Akteure der IT Mitglied sind, hat auf seiner Webseite in der Rubrik „DsiN für Verbraucher“ ebenfalls einen Artikel zu sozialen Netzwerken eingestellt[8]. Hier steht die Datensparsamkeit an erster Stelle gefolgt von der Vorsicht bei Kontaktanfragen und der Beachtung der Rechte Anderer sowie des Kinder-/Jugendlichen-Schutzes. Die Tipps bezüglich der Logins und der Einstellungen sind durchaus hilfreich, insbesondere, da hier der Verzicht auf „Social Logins“ hervorgehoben ist. Mit einer solchen Möglichkeit der vereinfachten Anmeldung bei Firmen über Social-Media-Profile werden „auch Nutzerdaten und -aktivitäten an die jeweilige Social-Media-Plattform übermittelt“. Auch wenn, wie Wiewiorra u.a. feststellen[9], „Zweifel an der Sicherheit der Systeme für viele Konsumenten ein wichtiger Grund sind, sich bei Onlinediensten oder Webseiten nicht via Facebook, Google oder durch andere (soziale) Netzwerke anzumelden“, hilft eine Verstärkung dieses Zweifels durch einen gezielten Hinweis sicher weiter. Vorschläge zum Prüfen von Einstellungen und Verknüpfungen zu anderen Apps runden den Beitrag von DsiN ab.

Ein Blick über die Grenze geht zunächst zu der von der EU geförderten österreichischen Initiative Saferinternet.at, die laut eigener Aussage „vor allem Kinder, Jugendliche, Eltern und Lehrende beim sicheren, kompetenten und verantwortungsvollen Umgang mit digitalen Medien“ unterstützt. Dort gibt es neben einer FAQ[10], die beispielsweise Alternativen zu WhatsApp auflistet und die Frage des Löschens von Profilen beantwortet, auch eine Reihe von Flyern zu verschiedenen Plattformen (TikTok, Snapchat, Instagram, Youtube und Facebook). Direkt an Kinder und Jugendliche richten sich die entsprechend gestalteten Flyer, während die „10 Tipps zum Thema Soziale Netzwerke für Kinder und Jugendliche“ für die Eltern gedacht sind und diese beispielsweise auffordern: „Machen Sie sich schlau“. Hier wird auch dazu aufgerufen die Kenntnisse der Kinder wertzuschätzen. Der Schweizer Datenschutzbeauftragte erläutert ebenso die Gefahren, die bei der Nutzung von sozialen Netzwerken drohen und gibt dann zehn Empfehlungen ab[11]. Diese zeigen einen interessanten weiteren Aspekt auf, wenn sie auffordern zu prüfen „ob Sie in einem Bewerbungsgespräch mit den entsprechenden Daten konfrontiert werden möchten“. Zur Sicherheit soll deshalb auch regelmäßig das Internet nach dem eigenen Namen und möglichen Profilen durchsucht werden. Die abschließenden Verweise auf weiterführende Informationen sind allerdings veraltet.

Aus der endlos scheinenden Liste der speziellen Datenschutz-Fachseiten seien nur einige ausgewählt. So hat die Seite www.datenschutz.org des VFR Verlag für Rechtsjournalismus allgemeine Informationen zusammengetragen[12]. Angesichts der grundsätzlichen Problematik des Datenschutzes bei sozialen Medien wird dort festgestellt, dass die Privatsphäre-Einstellungen „das A und O“ sind, damit der Datenschutz bei sozialen Netzwerken gewährleistet wird. Dafür, so wird gewarnt, sind „Selbstdisziplin und Zeitinvestment notwendig“. Darauf folgen Hinweise zu grundsätzlichen Überlegungen vor der Anmeldung (pro Netzwerk eine eigene E-Mail-Adresse wählen, Pseudonym nutzen, Profiltyp privat oder geschäftlich beachten), zu Einstellungen (Sichtbarkeit für Suchmaschinen/von Kontaktdaten/der Inhalte) sowie zu Rechten und Pflichten („Bleiben Sie sozial: Nicht nur Ihre Privatsphäre zählt“).

Der Medienratgeber www.schau-hin.info, eine Initiative des Bundesfamilienministeriums, öffentlich rechtlicher Sender und der AOK, hebt auf seiner Infoseite[13] auch die Chancen sozialer Medien hervor: Posts der Jugendlichen können demnach „Kreativität fördern“ und die „Auseinandersetzung mit der eigenen Identität, Inszenierungen und medialen Körperbildern“ anregen. Die dann folgenden allgemeinen Tipps appellieren vor allem an die Eltern, die die Einstellungen in den jeweiligen Netz-

werken restriktiv auf den Freundeskreis ihres Kindes beschränken sollen. Tiefergehende Analysen beziehen sich auf jeweils eine Plattform oder ein Thema (z. B. TikTok, Snapchat, medialer Körperkult) und werden durchaus konkret in den Ratschlägen. So werden etwa bezüglich Snapchat „Tipps für ein sicheres Einrichten" der App gegeben[14].

Die privacyxperts.de bezeichnen den Datenschutz bei sozialen Medien zumindest im Link als „umstrittenes Thema"[15]. Dann eröffnet diese Seite allerdings Unternehmen „das ein oder andere Hintertürchen in Sachen Social Media bzw. Onlinemarketing". Für die Nutzung der sozialen Netzwerke gibt es im Kern nur den Tipp: „Generell muss eben jeder, der Social Media aktiv nutzen möchte, abwägen, was er/sie von sich preisgeben möchte". Von „umstritten" bleibt auf diese Weise nicht sonderlich viel übrig.

Anders bei Kathrin Strauß, die als Datenschutzbeauftragte auf der Seite datenschutzexperte.de Klartext redet[16], wenn sie etwa konstatiert, dass Social-Media-Plattformen „im Grunde nur riesige Werbemaschinen" sind. Der Text verweist nicht nur auf das BSI, sondern erwähnt auch ausdrücklich, dass Metadaten von den Plattformen zur Profilbildung genutzt werden. Die Tipps reichen dann von Passwörtern über Privatsphäre-Einstellungen bis zu Kontaktanfragen und werden zum Teil konkret: „Machen Sie den von ihnen veröffentlichten Content (Postings, Storys etc.) nur für ausgewählte Freund:innen sichtbar".

Unerwarteterweise geben auch ganz andere Webseiten wie handicare-treppenlifte.at mitunter Tipps für die Nutzung sozialer Medien[17]. Zwar beschränkt sich in diesem Fall die Kritik auf die Erwähnung, dass alles Veröffentlichte „im Internet" bleibt, und den Hinweis „Geben Sie nur die personenbezogenen Daten ein, die auch wirklich notwendig sind" ohne diese Notwendigkeit zu spezifizieren. Positiv hervorzuheben ist allerdings der Schlussbereich der Seite, in dem über die üblichen hinaus weitere interessante Seiten für Senioren erwähnt werden.

Um überhaupt einen Überblick über die bereits hinterlassenen Daten zu bekommen lohnt sich ein Blick in die Empfehlung der Verbraucherzentrale „Facebook und Co: Finden Sie heraus, was Unternehmen von Ihnen speichern" aus dem Jahr 2020[18]. Hier wird konkret beschrieben, wie der Abruf der eigenen Daten bei Facebook, Instagram, WhatsApp, Google und Twitter funktioniert. Auf der Webseite wird außerdem für das klassische Verfahren der Anfrage per Post ein vorformulierter Musterbrief bereitgestellt. Vielleicht ist das eine Möglichkeit mit dem oben erwähnten „IT-Frühjahrsputz" des BSI ganz herkömmlich zu beginnen.

Zum Abschluss dieses Artikels seien nun die wichtigsten Hinweise für die Nutzung sozialer Medien aus den Quellen nochmals als konkrete Aufforderungen zusammengefasst:

- Wählen Sie nach Möglichkeit sehr enge Voreinstellungen bezüglich der Zugriffe auf Ihre Daten
- Achten Sie auf absolute Sparsamkeit bezüglich Ihrer Daten
- Verwenden Sie nach Möglichkeit ein Pseudonym statt Ihres Namens
- Seien Sie vorsichtig bei der Bestätigung von Kontaktanfragen (prüfen Sie die Echtheit)
- Schützen Sie auch die Rechte Anderer (bzgl. Bilddaten und bei Informationsweitergabe)
- Wählen Sie für jedes Netzwerk ein anderes, sicheres Passwort
- Schränken Sie die Sichtbarkeit des Profils auf den Freundeskreis ein und schließen Sie vor allem den Zugriff von Suchmaschinen aus

Darüber hinaus empfiehlt Mike Kuketz im kuketz-blog.de einige Web-Frontends und Apps, mit denen „datenschutzfreundlich die Inhalte" der jeweiligen Plattform wenn auch nicht geändert, so doch abgerufen werden können[19].

Trotz Beachtung all dieser Tipps sollten Sie irgendwann die Datenschutzbestimmungen, Allgemeinen Geschäftsbedingungen oder Nutzungsbedingungen eines jeden sozialen Netzwerks aufmerksam lesen. Und dann könnte die Zeit gekommen sein, im „IT-Frühjahrsputz" den einen oder anderen Account wieder zu löschen.

1 https://doi.org/10.48550/arXiv.2202.10543

2 https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Onlinekommunikation/Soziale-Netzwerke/Sichere-Verwendung/sichere-verwendung.html

3 https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Onlinekommunikation/Soziale-Netzwerke/soziale-netzwerke_node.html

4 https://www.bfdi.bund.de/DE/Buerger/Inhalte/Telefon-Internet/TelekommunikationAllg/DatenschutzInSozialenNetzwerken.html

5 https://www.datenschutz.de/datenschutz-in-sozialen-netzwerken/

6 https://www.ldi.nrw.de/soziale-netzwerke

7 https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/medienkompetenz/2018-BlnBDI-Broschuere_Soziale_Netzwerke.pdf

8 https://www.sicher-im-netz.de/sicher-unterwegs-sozialen-netzwerken

9 https://www.econstor.eu/handle/10419/227073

10 https://www.saferinternet.at/themen/soziale-netzwerke/

11 https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/Internet_und_Computer/onlinedienste/soziale-medien/erlaeuterungen-zu-sozialen-netzwerken.html#1816884822

12 https://www.datenschutz.org/soziale-netzwerke/

13 https://www.schau-hin.info/soziale-netzwerke

14 https://www.schau-hin.info/sicherheit-risiken/snapchat-sicher-einrichten-das-sind-die-risiken

15 https://www.privacyxperts.de/datenschutz-und-social-media-das-umstrittene-thema/

16 https://www.datenschutzexperte.de/blog/datenschutz-im-internet/datenschutz-in-sozialen-netzwerken-was-nutzer-beachten-sollten/

17 https://handicare-treppenlifte.at/uber-handicare/blog/10-tipps-zum-sicheren-umgang-mit-sozialen-netzwerken/

18 https://www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/facebook-und-co-finden-sie-heraus-was-unternehmen-von-ihnen-speichern-24684

19 https://www.kuketz-blog.de/empfehlungsecke/#soziale-netzwerke

Frans Valenta

Technische Innovationen aus China

Social-Media-Anbieter wie z. B. YouTube, Vimeo, Facebook, Instagram oder Twitch bieten Webstreaming als Option an, um den Nutzer-Kanal attraktiver erscheinen zu lassen. Veranstaltungen, Aufführungen, Versammlungen und besondere Ereignisse können so von Zuschauern auf einem Telefon, Computer oder über internetfähige TV gesehen werden. Hier kann meistens per Text-Kommentar eine Interaktion mit dem Publikum stattfinden.

Für die ersten Schritte zum Video-Streaming ins Internet reicht ein Smartphone oder Tablet aus. Wer höhere Ansprüche an die Bildqualität hat und mit mehreren zuschaltbaren Kameras oder anderen Signalquellen ein Publikum erreichen möchte, kann dies mit Laptops oder Desktop-Computern und Software wie OBS oder mit Videoschnitt-Hardware bewerkstelligen.

Wenn aber mal Impressionen eines Festivals im Freien in FullHD-Qualität eingefangen werden sollen, ist der technische Aufwand mit einem Computer nicht unerheblich.



Per HDMI an eine Kamera angeschlossene YoloBox. Bild: Frans Valenta

Die chinesische Firma YoloLiv hat für den mobilen Einsatz eine passende Lösung entwickelt. Das YoloBox[1] genannte Produkt besteht aus einem akkubetriebenen 8-Zoll-Monitor, der per HDMI-Anschlüssen mit bis zu zwei Kameras verbunden werden kann. An einem USB-Anschluss kann noch eine Webcam hinzugefügt werden. Über das Display kann die gewünschte Quelle für den Video-Stream und zusätzlich für eine Videoaufzeichnung auf eine SD-Karte angewählt werden. Die Verbindung zum Internet gelingt entweder über ein Netzwerkkabel, per W-LAN oder über die SIM-Karte eines Netzanbieters im dafür vorgesehenen Fach.

YoloLiv verspricht eine sehr einfache Bedienung. Für die Anmeldung bei YouTube werden „nur die Google-Zugangsdaten“ benötigt. Seltsam – bei anderen Geräten wie z. B. dem ATEM Mini von Blackmagic Design genügt die Angabe des Streamschlüssels und der Stream-URL. Die Google-Zugangsdaten abgeben bedeutet möglicherweise: Zugriff von YoloLive auf alle bei Google gespeicherten persönlichen Daten aller registrierten Smartphones, Tablets oder Computer. Betroffen sind dann unter anderem Kontakte, E-Mails, Fotos, Videos, Bewegungsprofile und Passwörter. Im Extremfall könnte YoloLiv den kompletten Account löschen.

Das Betriebssystem der YoloBox ist ein modifiziertes, stark beschränktes Android, das den Download eines Analysetools nicht zulässt. Es wäre interessant zu wissen, ob YoloLiv wenigstens auf eine OAuth-Authentifizierung zugreift, bei der die sensiblen Zugangsdaten nicht auf dem YoloLiv-Server landen sondern bei Google bleiben. OAuth (Open Authorization)[2] lässt zum Beispiel bei Facebook zu, dass Web-Anwendungen die hinterlegte E-Mail-Adresse abfangen und somit für Spam verwendet werden.[3] Der Schlusssatz zum OAuth-Artikel bei Wikipedia lautet: „Eran Hammer, ein bis dahin zentraler Redakteur der Spezifikation OAuth 2.0, verließ Ende Juli 2012 das Projekt, weil dessen Komplexität seiner Einschätzung nach von den meisten Softwareentwicklern kaum noch sicher implementierbar sei“. Eine Anfrage bei YoloLiv zu diesem Themenkomplex blieb bis zum Redaktionsschluss unbeantwortet.

Zur datenschutzfreundlichen Nutzung des Geräts sollte bei Bedarf jeweils ein Fake-Account angelegt werden, der keinerlei persönliche Daten enthält. In den Datenschutzbestimmungen von YoloLiv heißt es: *„Wenn Sie sich weigern, Ihre persönlichen Daten an YoloBox weiterzugeben, kann YoloBox Ihnen einige der Merkmale und Funktionen des YoloBox-Dienstes nicht zur Verfügung stellen. Sie können Ihre Benutzerinformationen und Einstellungen einsehen, aktualisieren, korrigieren oder löschen, indem Sie uns unter privacy@*

YoloBox.com kontaktieren" und *„YoloBox verwendet kommerziell angemessene physische, verwaltungstechnische und technische Sicherheitsmaßnahmen, um die Integrität und Sicherheit Ihrer persönlichen Daten zu bewahren. Bitte beachten Sie, dass keine Sicherheitsmaßnahmen perfekt oder unangreifbar sind. Wir können nicht garantieren, dass Ihre Daten nicht durch eine Verletzung unserer physischen, technischen oder verwaltungstechnischen Sicherheitsvorkehrungen zugänglich, offengelegt, verändert oder zerstört werden"*.

Dass die Verarbeitung der Daten nicht den europäischen Standards entspricht, zeigt diese Passage: *„Benutzer, die den YoloBox-Dienst aus der Europäischen Union oder anderen Nicht-US-Territorien besuchen, beachten bitte, dass alle Daten, die Sie in den YoloBox-Dienst eingeben, außerhalb der Europäischen Union oder eines anderen Nicht-US-Territoriums übertragen werden, um von YoloBox und seinen verbundenen Unternehmen für die hier beschriebenen Zwecke verwendet zu werden. Da YoloBox weltweit tätig ist, können wir die von uns gesammelten Informationen außerdem an weltweite Geschäftseinheiten und Tochtergesellschaften weitergeben. Durch die Bereitstellung von Daten über den YoloBox-Dienst stimmen Sie hiermit ausdrücklich einer solchen Übertragung Ihrer Daten in die Vereinigten Staaten oder andere Länder zu"*.[4]

Mit der alternativen Möglichkeit, Streams über ein RTMP-Protokoll zu verschicken, erübrigt sich die Notwendigkeit Account-Zugangsdaten preiszugeben. Aber ganz so einfach geht das nicht. Normalerweise würde man jetzt ein paar Eingabefelder für die notwendigen Parameter erwaten. Aber YoloLiv weist freundlich darauf hin, dass eine Nachricht an die angegebene E-Mail-Adresse mit den Hinweisen zur Eingabe der Daten verschickt wurde. Also mal auf dem Rechner oder Smartphone nachschauen, was da übermittelt wurde. Spyware? Ein Trojaner? Vielleicht ja nur eine Mail mit einem Script, damit YoloLiv an den Social-Media-Aktivitäten auf anderen Geräten partizipieren kann?

Eine erzwungene Produktanmeldung scheint bei chinesischen Technologie-Erzeugnissen üblich zu sein. Auch bei der YoloBox ist dies mit der verpflichtenden Erstellung eines YoloLiv-Accounts vor der Geräte-Nutzung der Fall. Leider wird in bestimmten Zeitintervallen eine erneute Anmeldung verlangt – vermutlich, „um in Kontakt zu bleiben". Damit ist wegen der Personalisierung das Verleihen oder Vermieten des Geräts praktisch ausgeschlossen.Wer will schon seine persönlichen (Fake-) Daten an Freunde oder Geschäftspartner verraten?

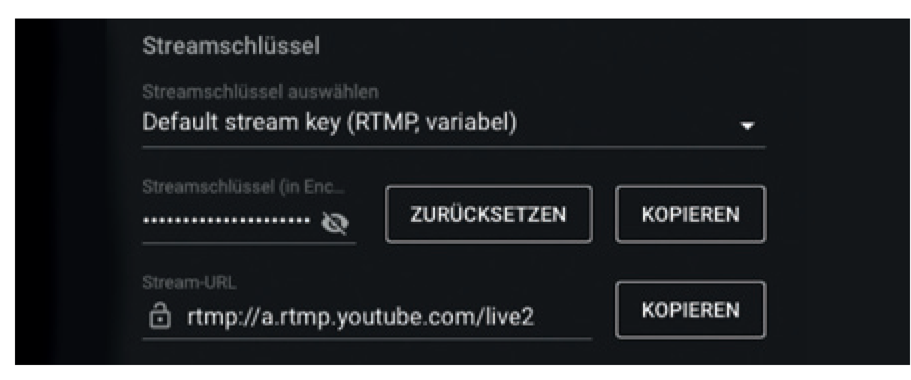
Die Kamera Osmo Pocket[5] der durch Drohnen und Gimbals für den Hobby- und Filmbereich bekannt gewordenen Firma DJI muss mithilfe der App „DJI Mimo"[6] aktiviert werden. Ohne Aktivierung ist die Kamera nicht funktionsfähig. Fast alle negativen Bewertungen auf Amazon zu dieser Kamera führen diesen Punkt auf. Oft ist an dem Android-Smartphone kein USB-C-Anschluss vorhanden oder die Android- bzw. iOS-Version ist inkompatibel. Dann gibt es nur zwei Möglichkeiten: entweder das Gerät zurückschicken oder ein neues Smartphone kaufen. Über den Sinn einer Aktivierung kann spekuliert werden. Da diese Geräte in China entwickelt wurden und auch in China verkauft werden ist anzunehmen, dass hier Vorgaben der chinesischen Regierung umgesetzt werden zu einer weit gefassten Kontrolle aller Medien-Aktivitäten.

Wenn der chinesischen App TikTok erlaubt wird auf das Fotoalbum zuzugreifen, bedeutet das, dass alle Fotos erfasst werden, die auf dem Handy gespeichert sind – und dabei sogar Gesichtszüge aller abgebildeten Personen per Gesichtserkennung identifiziert werden. Wenn der App erlaubt wird, auf den Standort zuzugreifen, bedeutet das, dass sie weiß, wo man sich aufgehalten hat.[7]



DJI Osmo Pocket. Bild: Frans Valenta

Es ist kaum anzunehmen, dass sich die Apps von YoloLiv oder DJI mit dem Sammeln von Daten zurückhalten. Laut der exodus-Datenbank[8] zeigt die DJI-Mimo-App diverse Tracker und unter anderem die Erlaubnis für Zugriff auf den Standort, das Netzwerk, die Accounts auf dem Gerät, die Kamera, das Mikrofon und die externe SD-Karte. Das sind ideale Voraussetzungen für eine genaue Foto-, Video- und Audioanalyse im Hintergrund mit der Legitimation zum „nach Hause telefonieren".



Für das Streamen auf YouTube wird nur ein Streamschlüssel und die Stream-URL benötigt.

1 https://yolobox.live/products/yolobox
2 https://de.wikipedia.org/wiki/OAuth
3 https://www.faz.net/aktuell/technik-motor/digital/login-mit-facebook-kann-gefaehrlich-werden-12860066.html
4 http://www.yololiv.com/site/privacy-policy
5 https://www.dji.com/de/pocket-2
6 https://www.dji.com/de/mimo
7 https://www.welt.de/politik/ausland/article203941694/Wie-China-mit-der-App-TikTok-Informationen-im-Netz-kontrolliert.html
8 https://reports.exodus-privacy.eu.org/de/reports/dji.mimo/latest/

Katrin Lowitz

Auswirkungen von zehn Jahren Newsfeed

Über die sozialen Medien ist die Welt im Ukraine-Konflikt live dabei. Twitter ist bereits ein interstaatlicher Kommunikationskanal geworden und hat die diplomatischen Depeschen abgelöst. In Krisenregionen funktionieren offizielle Kanäle, Zeitungen, Radio, Fernsehen oft nicht mehr, die sozialen Medien übernehmen diese Rolle. In einem Beitrag bei Focus-Online erläutert Gabor Steingart die positive Rolle der sozialen Medien im Informationskrieg um die Ukraine. Dabei verkennt er aber, dass Krisen in das algorithmische Beuteschema der sozialen Medien fallen. Emotionale Bilder und Videos, kurze knackige Texte befeuern das Klickverhalten und der Algorithmus spült einem die Ukraine-Nachrichten in die Timeline. Eine verängstigte Welt, deren erster Blick morgens dem Smartphone gilt, um zu überprüfen, ob die Ukraine noch existiert, steuert den Newsfeed. Der aktuelle, dramatische, schwer verständliche IPCC-Bericht über die bedrohliche Entwicklung der Klimakrise hat wieder einmal das Nachsehen.

Obwohl über den Newsfeed und das Zielgruppen-Targeting schon seit Jahren ausführlich und kritisch berichtet wird und die Plattformen wiederholt aufgefordert werden nachzubessern, hat sich an den Grundsätzen des Algorithmus nichts geändert. Die darin enthaltene Zersplitterung der Gesellschaft hat offline bereits massive Auswirkungen. Jeder lebt in seiner eigenen Realität. Egal wie die Plattform heißt, die Struktur der Informationssteuerung ist ähnlich. Die Aussteuerung des Verhaltens erfolgt jedoch aufgrund der Plattformlogik (Instagram, schöne Bilder), Twitter (kleinster Marktanteil in Deutschland, textlastig).

Meta erläutert dies in seinen Nutzungsbedingungen:

„Kapitel 1 Von uns angebotene Dienste.

Wir stellen dir ein personalisiertes Erlebnis bereit: Dein Erlebnis auf Facebook unterscheidet sich von dem aller anderen: Angefangen bei den Beiträgen, (….). Um dein Erlebnis zu personalisieren, verwenden wir die uns zur Verfügung stehenden Daten – beispielsweise über von dir hergestellte Verbindungen, Optionen und Einstellungen, die du wählst, und was du auf unseren Produkten sowie außerhalb dieser tust."

Das personalisierte Erlebnis fasst das Business-Modell von Meta zu einer Lookalike Audience für Werbetreibende zusammen.

„Zur Erstellung einer Lookalike Audience sucht unser System anhand von Informationen wie demografische Angaben, Interessen und Verhaltensweisen der Ausgangszielgruppe nach neuen Zielgruppen, die ähnliche Merkmale aufweisen. Wenn du eine Lookalike Audience einsetzt, wird deine Werbeanzeige an diese Zielgruppe ausgeliefert, die deinen Bestandskunden ähnelt."

Die mathematische Basis für diesen Erfolg lieferte Larry Page mit seiner Patentanmeldung vom 10. Januar 1997. Durch Backlinks und Klickverhalten der Nutzer werden die Inhalte in der Google-Suche hierarchisch sortiert. Google erklärt es heute so: „(…) Dazu gehören unter anderem die in deiner Suchanfrage verwendeten Wörter, die Relevanz und Nützlichkeit von Seiten, die Sachkenntnis von Quellen sowie dein Standort und deine Einstellungen. (….)"

Diese Maßnahmen fühlen sich perfekt an, alle Informationen werden für einen passend sortiert. Jeder hat seine ganz eigene Bibliothek, die Informationen, die einen am meisten interessieren, werden direkt präsentiert, die man nicht sehen möchte, werden in die hinteren Regale verbannt. In einer Welt, in der man sich auf allgemein anerkannte Grundsätze und wertebasierte Regeln geeinigt hat, an die sich alle halten, großartig.

Allerdings wird die Sortierung der Informationen, je nachdem, wer hier klickt, zu einem gesellschaftlichen Problem.

In einer im April 2019 von der Northwestern University durchgeführten Studie wurden die Facebook-Algorithmen auf auf Vorurteilen basierende Funktionsweise untersucht. Zu diesem Zweck wurden zwei Versuchsanordnungen für Wohnungsanzeigen und Stellenanzeigen erstellt, ohne Einschränkungen für Frauen und Männer oder Kaukasier und People of Color. Da der Algorithmus die Anzeigen trotzdem auf Klickwahrscheinlichkeit der einzelnen Nutzer ausspielt, kommt es zu einer Selbstbeschränkung von Möglichkeiten. Beispielhaft klicken Kaukasier eine Anzeige, in der People of Color in einem Haus gezeigt werden, seltener an, wie auch umgekehrt (unbewusste Vorurteile „das ist nicht für mich!"). Wenn in der Anzeige keine Menschen gezeigt werden, ist die Klickwahrscheinlichkeit ausgeglichen. Die (un)bewussten Vorurteile im Menschen formen den Algorithmus. Dies lässt sich nicht verhindern, solange Inhalte nach dem persönlichen Nutzerverhalten strukturiert sind.

Mit der Nutzung von verhaltensbasiertem Targeting in Wahlkämpfen bekamen die sozialen Medien eine gesellschaftlich hochkritische Bedeutung.

Soziale Medien in der Politik

Sowohl die Ergebnisse der Wahl zum BREXIT als auch die US-Präsidentschaftswahl 2016 sorgte am Wahltag für Überraschungen. Durch die Intransparenz im Online-Wahlkampf bleibt der Einblick in den Diskurs der Andersdenkenden versperrt. Vor den Zeiten des Online-Wahlkampfes konnte man sich an einen Kiosk stellen und diverse Zeitungen aufschlagen und erhielt eine Übersicht über die Stimmung des politischen Gegners, gute Zeitungen haben dies sogar für die Leser aufbereitet.

Whistleblower **Christopher Wylie** veröffentlichte am 17.03.2018 im britischen Guardian, wie Cambridge Analytica (CA) seine politischen Kunden weltweit bediente. Die Mitarbeiterin von CA, **Brittany Kaiser**, führte dies in ihrem Buch „die Datendiktatur" noch weiter aus. In der Netflix-Doku „The Great Hack" von Juli 2019 kann man in

die Tiefen der Nutzerdatensammlung eintauchen. In der Doku „The Social Dilemma" kann man sich vorführen lassen, wie gezielt jede beliebige Werbung durch Facebook ausgespielt wird.

Etliche Anhörungen, vor Ausschüssen des US-Kongresses und -Senats, sowie vor dem Britischen und dem EU-Parlament, später und nach Beteuerungen der Plattformbetreiber zur Besserung wurde von YouTube, Twitter und Facebook sehr viel Geld in die Content-Moderation und das Säubern der Inhalte gesteckt.

Laut eigenen Angaben hat Facebook seit 2016 etwa 13 Milliarden Dollar in Technik und Personal gesteckt, um die Content-Moderation zu verbessern. Auch die Anzahl der Mitarbeiter hat sich auf 40.000 Personen erhöht. In 2021 hat sich eine weitere Whistleblowerin in den Dienst der Allgemeinheit gestellt. Frances Haugen hat Tausende von internen Dokumenten, die FacebookFiles, über das Wallstreet Journal veröffentlicht. In der Anhörung sagte sie u.a. dazu aus, dass lediglich 9% der Facebook-Nutzer in Englisch unterwegs sind, allerdings wird 87% des Budgets für Content-Moderation in englischsprachigen Regionen ausgegeben. Das würde bedeuten, bei einer global angemessenen Content-Moderation müsste sich das Budget dafür verzehnfachen.

In Anhörungen legte **Mark Zuckerberg** irreführend dar, dass Facebook 90% der HateSpeech mit Artificial Intelligence aufspürt, der Rest wird von Content-Moderatoren beseitigt. Betrachtet man das bezogen auf die tatsächlich vorhandene Hassrede im Netz, geht Facebook in den internen Dokumenten von ca. 3-5% Hate Speech aus, die von ihrer AI überhaupt erkannt wird.

Gerade Staaten, die keine funktionierende freie Medienlandschaft haben, werden alleine gelassen. Nobelpreisträgerin **Maria Ressa**, Herausgeberin des Online-Magazins Rappler von den Philippinen, hat bereits 2016 Facebook gewarnt, wie politischer Wahlkampf mit Desinformation geführt wurde und Facebook ist nicht eingeschritten. Entwicklungsländer sind dem Silicon Valley einfach egal. Die Auswirkung dieser Missachtung erfahren wir in einer weiteren politischen Destabilisierung von Entwicklungsländern, die eine unterentwickelte freie Presse und geringe demokratisch etablierte Prozesse haben:

- Brasilien: Podcast von HumaneTech „Down the Rabbit Hole by Design mit Guillaume Chaslot" ehemaliger YouTube Mitarbeiter u.a. über den Wahlkampf per YouTube von Präsident Jair Bolsonaro in Brasilien
- Myanmar: Die Rolle von Facebook bei der Vertreibung der Rohingya
- Indien: Facebook durch Enthüllungen zu Gewaltaufrufen unter Druck

Demokratie und Meinungsfreiheit

Eines der bekanntesten Zitate über die Demokratie ist von Winston Churchill: „No one pretends that democracy is perfect or all-wise. Indeed, it has been said that democracy is the worst form of government except all those other forms that have been tried from time to time."

Den Sozialen Medien wird bis heute grundsätzlich positiv unterstellt, dass sie bereichernd für den Diskurs und die Meinungsfreiheit sind, daher wird an der Nutzung der Plattformen von vielen öffentlichen Einrichtungen, Medien, Universitäten und Non-Profits festgehalten. Dabei sollte man gleichfalls unterstellen, dass alle Meinungen gleich gehört werden. Die Algorithmen der Plattformen steuern aber vorwiegend Text- und Bildmaterial so aus, dass die von Menschen geklickten „Clickbaits" häufiger in der Timeline der Nutzer auftauchen. Leider führt das nicht dazu, dass die beste Information gezeigt wird, sondern diejenige, die bei den Menschen den emotionalen Trigger anspricht. Zwei Studien haben das untersucht und bestätigt: „Emotion shapes the diffusion of moralized content in social networks" vom 26. Juni 2017 sowie „Out-group animosity drives engagement on social media" vom 23. Juni 2021.

Das hat weitreichende Folgen auch für die unter finanziellem Druck stehende Medienlandschaft, die sich diesen Regeln anpasst und Überschrift und Teaser möglichst aufregend gestaltet, um ihrerseits Clickbait zu erzeugen.

Für Akteure, die mit Desinformation finanzielle oder politische Gewinne über die Plattformen anstreben, ist es umso einfacher sich dieser einfachen Logik zu bedienen. Facebook hat dabei das größte Problem, da es die größte Reichweite hat und für jeden, der manipulieren will, egal ob positiv oder negativ, Lüge oder Wahrheit, Konsum oder Politik, sehr attraktiv ist.

Forschung, Studien, Informationen, die mehr als 5 Minuten Beschäftigung benötigen, sind erheblich benachteiligt die Allgemeinheit zu erreichen. Natürlich bilden sich auch in den sozialen Medien die Wissenschaftsblasen aus, so dass dies nicht wirklich wahrgenommen wird.

Facebook ist „biased against facts", sagt Nobelpreisgewinnerin Maria Ressa.

Mentale Gesundheit

Über die Auswirkungen auf die mentale Gesundheit bei dem Konsum von sozialen Medien wird international umfassend geforscht. Spätestens mit der Veröffentlichung der internen Dokumente aus dem Konvolut von **Frances Haugen** liegen die Beweise aufgrund der internen Daten von Facebook vor. Auch andere haben vorher schon umfassend auf die mentalen Auswirkungen nicht nur bei den Sozialen Medien, sondern auch bei Google-Anwendungen aufmerksam gemacht.

Jonathan Haidt, Sozialpsychologe an der New York Universität, hat seine Untersuchungen zu den Auswirkungen auf Teenager und die Generation-Z in The Atlantic im April 2022 veröffentlicht: „Why the Past 10 Years of American Life Have Been Uniquely Stupid." Vielleicht sind manche Länder davon geringer betroffen, trotzdem hat das in einer globalisierten Welt Auswirkungen.

Bereits 2014 hat ein ehemaliger Googler davon berichtet, wie die Tech-Industrie die Plattformen so entwirft, dass möglichst lange Nutzungszeiten entstehen und damit auch die Werbeeinnahmen vergrößert werden können: „How better tech could protect us from distraction" so **Tristan Harris**, Gründer der HumaneTech Community im Dezember 2014 bei TEDx Brussels sowie „Dopamine, Smartphones & You: A battle for your time" vom 1. Mai 2018 im Blog der Harvard Universität.

All die Jahre später hat sich trotzdem nicht viel geändert. Insider haben ausgepackt, Journalisten recherchiert, Datenwissenschaftler geforscht, Sozialpsychologen in vielen Ländern die Auswirkungen auf die mentale Gesundheit untersucht. Und immer noch besteht

die Erwartung an die Sozialen Medien, dass sie dieses Problem irgendwie lösen könnten. Trotz der Beteuerungen der CEOs in den Anhörungen, dass an dem Problem hart gearbeitet wird, sind Facebook und Twitter weit davon entfernt das Problem zu lösen – und sie werden es mit diesem algorithmischen Modell nie lösen.

Das Versprechen der Plattformbetreiber, dass künstliche Intelligenz die Content-Moderation erfolgreich umsetzen kann, hat sich schon längst in hohle Phrasen aufgelöst. Nicht einmal die Menschen sind in der Lage Polemik, Satire, Zynismus eindeutig in einem Text zuzuordnen.

Darüber hinaus ist eine Welt, in der private Unternehmen mit intransparenten Algorithmen darüber entscheiden, welche Informationsinhalte veröffentlicht werden und welche nicht, höchst problematisch und nicht erstrebenswert.

Trotz aller Informationen zu den negativen Effekten dieser Plattformen, die darauf beruhen, dass eine kleine Minderheit den Diskurs beherrscht, nutzen fachkundige Organisationen weiterhin die Sozialen Medien. Angefangen bei der Bundesregierung mit den Logos auf ihren Webseiten ist dies kostenlose Werbung und öffentliche Unterstützung dieser Dienste. Erfolg als Reichweite ist über diese natürlich einfach zu tracken, mit jedem Follower und Like gibt es wieder „Dopamin-Cookies" für die Mitarbeiter der Marketingabteilung.

Was nun?

Momentan sind gerade mal ca. 66% der Menschen weltweit online. Neben den inhaltlichen Problemen der Informationsverteilung sind auch die Energieressourcen, die das Internet verbraucht, erheblich. Obwohl die Entwicklungsländer ein Recht auf Zugang zu den digitalen Märkten haben, halten wir an unserem Anspruch zum endlosen Streamen, Gamen und Konsumieren von digitalen Inhalten fest. Das Öko-Institut hat den Ressourcenverbauch unseres digitalen Lebens berechnet, incl. Bereitstellung der zugehörigen Data-Center und Geräte.

In allen Lebensbereichen sind Reduzierungen an Komfort und Konsum erforderlich, um die Klimakrise aufzuhalten, warum nicht auch bei der Digitalisierung von Online-Angeboten? Ist das wirklich ein Einschnitt, wenn wir nicht mehr eine Flut von Bildern und Videos posten können? Wenn wir nicht mehr tagelang MMORPG (Massive Multiplayer Online Role-Playing Games) spielen können?

Die EU hat neue Regelungen für die Digitalen Märkte und Services sowie für die Anwendungen von Künstlicher Intelligenz in Plattformen und Produkten ausgegeben. Um die eigentliche Frage **„Wofür brauchen wir das Internet?"** hat sie sich weiterhin gedrückt. In einer Welt mit beschränkten Ressourcen sind diese im digitalen Leben ebenfalls notwendig. Wir müssen uns entscheiden, wofür wir das Internet nutzen wollen.

Barack Obama hat in seiner Keynote am 21. April 2022 in Stanford einen ersten Ausblick darauf gegeben, den ich unterstützen kann: „The internet is a tool. Social media is a tool. At the end of the day, tools don't control us. We control them. And we can remake them. It's up to each of us to decide what we value and then use the tools we've been given to advance those values."

Die internationale Gemeinschaft muss sich darauf verständigen, welche Inhalte in einer Gesellschaft online bereitgestellt werden sollen. Wer sich mit den Nachhaltigkeitszielen der Vereinten Nationen schon einmal beschäftigt hat, wird feststellen, dass sie weitestgehend unser gesamtes Leben umfassen. Das wäre ein guter Anfang.

Die verhaltensbasierte Sortierung von Informationen hat sich als ein großer Fehler erwiesen. Der Run auf eine neue Art der Suchmaschine ist wieder eröffnet. Trotzdem müssen wir uns fragen, ob wir den Aufmerksamkeitswettbewerb zwischen Katzenvideos und Forschungsinformationen beibehalten wollen.

Es ist eine vertikale und eine horizontale Struktur zur Sortierung von Informationen erforderlich. Wichtig ist dabei vor allem die Herkunft der Informationen. Auch im Internet gilt, dass für Informationen der Herausgeber die Verantwortung übernehmen muss. Das hat nichts mit der Beschränkung der Meinungsfreiheit zu tun. Wer im analogen Leben mit seiner Meinung unterwegs ist, muss sich ebenfalls einer unerwünschten Reaktion stellen.

Informationen von öffentlichen Stellen oder Bildungs- und Forschungseinrichtungen sollten sich nicht mit Desinformation von anonymen Konten herumschlagen müssen. Wer sich als Privatperson in einem Diskurs üben will, kann einer Organisation, einer politischen Partei oder einem Verein beitreten oder ein Ehrenamt übernehmen und dort sein Recht auf Meinungsfreiheit ausüben.

Die menschlichen Erfahrungen in so einem Umfeld wiegen 10 Jahre Posten und Tweeten wieder auf.

Leseliste

Sheera Frenkel, Cecilia Kang, Inside Facebook: die hässliche Wahrheit 2021

Roger McNamee, Zucked, Waking Up to the Facebook Catastrophe 2019

Shoshana Zuboff, Das Zeitalter des Überwachungskapitalismus 2018

Dr. Safiya Umoja Noble, Algorithms of Oppression: How search Engines Reinforce Racism 2018

Cathy O'Neill, Angriff der Algorithmen, Wie sie Wahlen manipulieren, Berufschancen zerstören und unsere Gesundheit gefährden 2017

Steven Levy, Google Inside 2011

Klaus-Jürgen Roth

Europa reguliert mit dem Digital Services Act das Internet



Bild: iStock.com/ sesame

Die Verhandlungsführer des EU-Parlaments, des Ministerrats und der Brüsseler Kommission haben sich in der Nacht zum 23.04.2022 nach einer knapp 16-stündigen Marathonrunde auf einen Kompromiss für den Digital Services Act (DSA) verständigt. Wahlweise gilt der DSA seinen Machern als „Goldstandard" für die Internetregulierung, Ende des „Wilden Westens" im Cyberspace, in dem sich die Tech-Giganten Amazon, Facebook, Google & Co. ihre eigenen Regeln schufen, oder gar als „digitales Grundgesetz" oder „Grundgesetz fürs Internet".

Kommissionspräsidentin Ursula von der Leyen (CDU) betonte bei der Bekanntgabe des erzielten Kompromisses: „Er wird dafür sorgen, dass das Online-Umfeld ein sicherer Raum bleibt, der die freie Meinungsäußerung und Möglichkeiten für digitale Unternehmen schützt." Je größer die Plattform sei, desto größer auch die Verantwortung des Betreibers.

- Anwendungsbereich

In den Anwendungsbereich des DSA fallen verschiedene Online-Vermittlungsdienste. Ihre Verpflichtungen hängen von ihrer Rolle, ihrer Größe und ihrem Einfluss auf das Online-Ökosystem ab. Vermittler nach dem Gesetz sind etwa Betreiber sozialer Netzwerke wie Meta mit Facebook und Instagram, Twitter und TikTok, andere Services zum Teilen von Inhalten wie YouTube, Suchmaschinen wie Google, Betreiber von App-Stores wie Apple und Online-Marktplätze wie Amazon und eBay. Erfasst werden ferner Vermittlungsdienste mit Netzinfrastruktur wie Internet-Zugangsanbieter, Domain-Registrierungsstellen und Hosting-Dienste wie Cloud-Anbieter und Webhoster.

Sehr große Online-Plattformen und sehr große Online-Suchmaschinen werden strengeren Anforderungen unterworfen. Dabei handelt es sich um Services, die mehr als zehn Prozent der 450 Millionen Verbraucher in der EU zu ihren Nutzern zählen beziehungsweise erreichen.

Um die Entwicklung von neu gegründeten Firmen und Startups im Binnenmarkt zu gewährleisten, werden laut dem Rat „Kleinst- und Kleinunternehmen" mit weniger als 45 Millionen monatlich aktiven Nutzern in der EU von bestimmten Vorschriften befreit.

Alle erfassten Online-Dienste müssen eine Kontaktstelle beziehungsweise einen Rechtsvertreter in der EU benennen. Das gilt auch für Messenger-Services wie Telegram, mit dessen Erreichbarkeit sich die deutsche Politik und Justiz derzeit schwertut (Roth, DANA 1/2022, 12 ff.). Niemand soll so in Europa auf dem Markt agieren können ohne sich an europäisches Recht zu halten.

- Illegale Inhalte

Die Verordnung verleiht laut der EU-Kommissionspräsidentin dem Grundsatz praktische Wirkung, „dass das, was offline illegal ist, auch online illegal sein sollte". Dies hatten zuvor auch die für Digitales zuständige Kommissionsvizepräsidentin Margrethe Vestager und die Berichterstatterin des EU-Parlaments, Christel Schaldemose von den Sozialdemokraten, immer wieder hervorgehoben. Neu ist diese Absage an die „Unabhängigkeitserklärung" für den Cyberspace früher Internetutopisten freilich nicht und eigentlich eine Binsenweisheit, die im Prinzip schon immer galt. Der „Cyberraum" war nie völlig vogelfrei jenseits der physikalischen Welt.

Der DSA sieht Maßnahmen zur Bekämpfung illegaler Waren, Dienstleistungen und Inhalte im Internet vor. Dazu gehört ein Mechanismus, der es den Nutzern ermöglichen soll entsprechenden Content einfach zu markieren und so zu melden. Plattformen können dabei mit „vertrauenswürdigen Markierern" („trusted flaggers") zusammenarbeiten.

Laut der zunächst in Grundzügen getroffenen Übereinkunft sollen Behörden aller Art künftig Host-Providern ohne Richtervorbehalt grenzüberschreitende Anordnungen schicken können, um gegen illegale Inhalte wie strafbare Hasskommentare, Darstellungen sexuellen Kindesmissbrauchs oder die unautorisierte Nutzung urheberrechtlich geschützter Werke vorzugehen. Betroffene Plattformen müssen solche Angebote dann „ohne unangemessene Verzögerung" sperren oder blockieren und bei schweren Straftaten zudem der Polizei melden. Maßnahmen zur Entfernung von Inhalten sollen nach dem Prinzip „Notice and Action" funktionieren.

Die Bestimmungen beziehen sich auch auf schädliche Inhalte wie Desinformation. Darauf zielen vor allem Auflagen für Empfehlungssysteme ab, die Plattformen etwa in ihren News-Feeds verwenden. Mit dem DSA müssen sie die Funktionsweise der dafür genutzten Algorithmen in groben Zügen transparent machen.

Dazu kommen neue Pflichten zur Rückverfolgbarkeit gewerblicher Nutzer auf Online-Marktplätzen. Alle Händler müssen identifiziert werden, während die Anonymität der privaten Nutzer gewahrt bleiben soll. Online-Marktplätze müssen Datenbanken auch Dritter stichprobenartig auf illegale Produkte abfragen und „zumutbare Anstrengungen" unternehmen, um die Rückverfolgbarkeit der Händler sicherzustellen.

Bei grenzüberschreitenden Sachverhalten soll mit dem Gesetz für digitale Dienste die Wirkung einer Anweisung gegen illegale Inhalte in der Regel auf das Hoheitsgebiet des anordnenden EU-Lands beschränkt werden. Die EU-Gremien wollen sicherstellen, dass Nutzern und den betroffenen Firmen Rechtsbehelfe zur Verfügung stehen. Diese sollen die Wiederherstellung von Inhalten einschließen, die fälschlicherweise als rechtswidrig angesehen und entfernt wurden.

Im Kontext der „russischen Aggression in der Ukraine und den besonderen Auswirkungen auf die Manipulation von Online-Informationen" fügten die Verhandlungsführer dem Text eine Klausel hinzu, die einen Krisenreaktionsmechanismus einführt. Dieser soll von der Kommission auf Empfehlung des geplanten Gremiums der nationalen Koordinatoren für digitale Dienste aktiviert werden. Ziel ist es die Auswirkungen der Aktivitäten von sehr großen Plattformen auf die entsprechende Krise zu analysieren und über „verhältnismäßige und wirksame Maßnahmen zu entscheiden, die zur Wahrung der Grundrechte zu ergreifen sind".

Das Parlament setzte sich für einen Artikel zum bildbasierten sexuellen Missbrauch auf Porno-Plattformen ein. Nutzer sollten Bilder, Videos oder Texte auf Erotik-Portalen wie Pornhub und xHamster erst hochladen dürfen, wenn sie beim Betreiber eine E-Mail-Adresse und Mobilfunknummer hinterlegt haben. Sexarbeiterinnen waren dagegen, da sie um die Anonymität und den Datenschutz besonders verletzlicher Gruppen im Netz fürchteten. Laut dem EU-Abgeordneten (MdEP) Patrick Breyer (Piratenpartei) konnte „das wahllose Sammeln der Handynummern" verhindert werden.

MdEP Geese als Initiatorin des Vorschlags bedauert eine Niederlage an diesem Punkt: „Leider bleibt der DSA an dieser Stelle blind. Wir haben es nicht geschafft wirksame Mittel zum Schutz vor geschlechtsspezifischer Gewalt im Internet zu verankern." Es gebe letztendlich auch keine eigene Klausel, die gegen Racheaktionen von Ex-Partnern mit Nacktbildern („Revenge Porn") oder gegen heimlich gemachte Aufnahmen etwa auf Festivals, schütze. Kommen wird aber etwa ein einfacher Meldemechanismus für „Racheepornos".

Hinsichtlich der Frage, inwieweit Meinungsfreiheit und andere Grundrechte tatsächlich geschützt werden, gehen die Ansichten auseinander. Allgemeine Geschäftsbedingungen (AGBs) und Gemeinschaftsstandards, die Regeln für die Moderation von Inhalten aufstellen, müssen in Zukunft laut Artikel 12 auf objektive und nicht-willkürliche Art und Weise angewendet werden. Eine ungleiche Behandlung gleicher Inhalte bei verschiedenen Nutzern wird damit rechtswidrig. Online-Dienste müssen ferner bei der Anwendung ihrer AGBs die Grundrechte ihrer User berücksichtigen.

Patrick Breyer monierte: „Die freie Meinungsäußerung im Netz wird nicht vor fehleranfälligen Zensurmaschinen (Upload-Filter), willkürlicher Plattformzensur sowie grenzüberschreitenden Löschanordnungen aus illiberalen Mitgliedsstaaten ohne Richterbeschluss geschützt, sodass völlig legale Berichte und Informationen gelöscht werden können." Die Privatsphäre im Netz werde entgegen der Position des Parlaments weder durch ein Recht auf anonyme Internetnutzung noch durch eines auf Verschlüsselung oder ein Verbot von

Vorratsdatenspeicherung aufrechterhalten. Industrie- und Regierungsinteressen hätten sich gegen digitale Bürgerrechte durchgesetzt.

Nach dem deutlich weniger breit ausgerichteten deutschen Netzdurchsetzungsgesetz NetzDG müssen Betreiber großer Plattformen für nutzergenerierte Inhalte bisher offensichtlich strafbare Beiträge, die ihnen beispielsweise User melden, innerhalb von 24 Stunden löschen. Die Entscheidung über komplexe Fälle, bei denen die potenzielle Rechtswidrigkeit schwer zu bewerten ist, können Anbieter seit zwei Jahren aber auch zunächst an die Freiwillige Selbstkontrolle Multimedia-Diensteanbieter (FSM) weiterleiten. Das dort angesiedelte Expertengremium muss sich vor allem mit Beleidigung und Agitation auseinandersetzen. Wenn die Vorschriften aus dem DSA spätestens Anfang 2024 greifen, haben sie in ähnlich gelagerten Bereichen direkt Vorrang gegenüber dem NetzDG.

- Transparenz und Verantwortlichkeit

Die Bestimmungen beziehen sich auch auf schädliche Inhalte wie Desinformation. Darauf zielen vor allem Auflagen für Empfehlungssysteme ab, die Plattformen etwa in ihren News-Feeds verwenden. Mit dem DSA müssen sie die Funktionsweise der dafür genutzten Algorithmen transparent machen. Ferner sollen sehr große Online-Portale für automatisierte Entscheidungen stärker zur Rechenschaft gezogen werden.

Über den Umgang mit rechtswidrigen und schädlichen Inhalten müssen Betreiber in maschinenlesbaren Transparenzberichten jährlich Rechenschaft ablegen. Sehr große Plattformen müssen zudem offenlegen, wie viel Personal sie für diese Moderationstätigkeiten einsetzen und wie dieses geschult und unterstützt wird. Alexandra Geese, Schattenberichterstatterin der europäischen Grünen-Fraktion, freut sich: „Das ist ein starker grüner Erfolg."

Zu den erfassten digitalen Services gehören Vermittlungsdienste wie Internetprovider und Domain-Registrierstellen. Eingeschlossen sind also auch soziale Netzwerke wie Facebook, YouTube, Twitter und TikTok, E-Commerce-Anbieter sowie Cloud- und Webhoster. Ihre Pflichten variieren je nach Rolle, Größe und Auswirkungen. Für kleine Unternehmen sind Ausnahmen vorgesehen.

- Microtargeting

Ein weiteres Kernelement des DSA sind aktualisierte Haftungsvorschriften und Regeln für personalisierte Reklame. Eine fraktionsübergreifende Koalition, Bürgerrechtler sowie Teile des Mittelstands drängten insofern auf ein weitgehendes Verbot von „spionierender Werbung" mit Microtargeting, was aber nicht Ergebnis des Kompromisses wurde. Nutzer sollen aber eine bessere Kontrolle darüber erhalten, wie ihre persönlichen Daten verwendet werden. Gezielte Werbung wird verboten, wenn es um sensible Daten geht, etwa aufgrund von sexueller Orientierung, Religion und ethnischer Zugehörigkeit. Dies bezieht sich auf Plattformen mit Nutzerinhalten wie Facebook, Instagram oder eBay, nicht aber auf Portale mit selbst erstelltem Content wie Nachrichtenseiten. Für Minderjährige gilt „ein vollständiges Verbot" personalisierter Anzeigen.

Das Prinzip des Überwachungskapitalismus, wonach Plattformen umfassende Datenprofile über Personen erstellen, soll so etwas eingeschränkt werden. Die Volksvertreter wollten weitergehende „Do not Track"-Einstellungen im Browser gesetzlich verankern, konnten sich damit aber nicht durchsetzen.

- Gegen Dark Patterns

Enthalten ist ferner eine Klausel gegen Design-Tricks wie „Dark Patterns": Online-Plattformen und -Marktplätze sollen Besucher nicht dazu drängen ihre Dienste zu nutzen, indem sie etwa eine bestimmte Wahlmöglichkeit stärker in den Vordergrund stellen oder den Empfänger durch störende Pop-ups umzustimmen versuchen. Darüber hinaus sollte die Kündigung eines Abonnements für einen Dienst genauso einfach sein wie die Anmeldung.

Die derzeitigen nervigen Cookie-Banner fallen nicht weg, könnten aber etwas „nutzerfreundlicher" werden. Derzeit drängen Webdesigner User mit Tricks wie „Dark Patterns" oft auf unfaire Art zu Entscheidungen. Bei Cookie-Bannern ist die Option für das Einwilligen etwa farblich deutlich unterlegt und direkt anklickbar, während für Opt-out mehrere Klicks nötig sind. Nutzer werden auch wiederholt belästigt, nachdem sie ihre Zustimmung in Tracking verweigert haben. Damit soll über ein Verbot im DSA Schluss sein: Schaltflächen müssen fair gestaltet sein, sodass Anwender künftig eine echte Wahl haben.

MdEP Geese bedauert, dass der Text in der finalen Verhandlungsrunde abgeschwächt worden ist. Bereits von bestehender Verbraucher- und Datenschutzgesetzgebung abgedeckte Praktiken seien so nicht mehr in diesem Verbot enthalten. Laut Kontrolleuren muss bei Cookie-Bannern schon jetzt anhand der Datenschutz-Grundverordnung (DS-GVO) auch ein „Alles-ablehnen-Button" zum Standard werden.

Marktplätzen wie Amazon oder eBay legen die EU-Gesetzgeber eine Sorgfaltspflicht gegenüber den Verkäufern auf, die Produkte oder Dienstleistungen über ihre Plattformen vertreiben. Sie müssen insbesondere Informationen über die verkauften Produkte und Dienstleistungen sammeln und anzeigen, um sicherzustellen, dass die Verbraucher angemessen informiert werden.

- Algorithmenkontrolle und Kennzeichnungspflicht

Sehr große Plattformen und Suchmaschinen gelten als relevant für die öffentliche Meinungsbildung und so auch für die Demokratie. Artikel 26 verpflichtet Online-Plattformen, die über 45 Millionen EU-Bürgerinnen und -Bürger erreichen, zu jährlichen Bewertungen der Risiken, die auf ihr Design einschließlich ihrer algorithmischen Systeme und ihrer Funktionsweise sowie auf die Nutzung ihrer Dienstleistungen für Grundrechte, Menschenwürde, Datenschutz, Meinungs- und Medienvielfalt, Diskriminierungsverbot, Jugendschutz und Verbraucherschutz zurückgehen. Eventuelle negative Auswirkungen der Services für den öffentlichen Diskurs und Wahlen, für geschlechtsspezifische Gewalt sowie für das mentale und physische Wohlergehen der Nutzer müssen von den Betreibern analysiert werden. Artikel 27 verpflichtet sie die identifizierten Gefahren auch zu beheben.

Die Kommission und Vertreter der Mitgliedstaaten sollen auch „Zugang"

zu den Algorithmen sehr großer Online-Plattformen haben. Wie weit dieser gehen soll, ist noch unklar. Veröffentlichen müssen werden Facebook & Co. ihre einschlägigen Programmroutinen wohl kaum, da sie hier immer wieder Geschäftsgeheimnisse ins Feld führen. Sie sollen ihre Daten und Angaben zu Algorithmen mit Behörden, Forschern und zivilgesellschaftlichen Organisationen teilen, damit ihre Arbeitsweise überprüft und ein Lagebild erstellt werden kann. Internetriesen wie Google und Facebook müssen auch eine öffentlich verfügbare Datenbank einrichten mit Informationen darüber, wer über ihre Werbenetzwerke wann mit welcher Anzeige angesprochen wurde.

Im Fall von Krisen wie Kriegen und Pandemien, von denen eine Gefahr für die öffentliche Sicherheit oder die menschliche Gesundheit ausgeht, kann die Kommission sehr große Plattformen auffordern dringende Bedrohungen auf ihren Portalen zu begrenzen. Diese spezifischen Maßnahmen sind auf drei Monate begrenzt.

Entdeckt eine sehr große Plattform Deepfakes, also manipulierte Bild-, Audio- oder Videoinhalte zum täuschend echten Nachahmen einer Person, muss sie diese entsprechend kennzeichnen. Solche Netzwerke sollen auch ein alternatives Empfehlungssystem anbieten, das nicht auf Profiling basiert.

- Aufsicht, Sanktionen und Inkrafttreten

Aufsichtsbehörden können Strafzahlungen in Höhe von bis zu 6% des weltweiten Jahresumsatzes eines Unternehmens verhängen. Auf Basis der Zahlen von 2021 betrüge die Höchststrafe für Amazon etwa bis zu 26 Milliarden Euro. Im Fall anhaltender Verstöße sind periodische Geldbußen in Höhe von bis zu 6% möglich. Regulierer können auch einstweilige Maßnahmen anordnen und Firmen auf bindende Selbstverpflichtungen einschwören. Sehr große Plattformen sollen über Gebühren an der finanziellen Last ihrer eigenen Aufsicht nach dem Verursacherprinzip mit bis zu 0,05% ihres weltweiten Jahresumsatzbeteiligt werden.

Die Kommission wird die zentrale Aufsicht über die speziell für sehr große Plattformen geltenden Vorschriften führen, um einen „Durchsetzungsstau" in einzelnen EU-Ländern zu verhindern. Die Regelung erweist sich als Arbeitsbeschaffungsprogramm. Die EU suchte bereits vor der endgültigen Einigung zum DSA IT-Experten für ihr Überwachungsgremium, das mit den nationalen „Digital Services Coordinators" zusammenarbeitet. Ein Fehler wie bei der DSGVO soll so verhindert werden, wo Irland als Flaschenhals beim Verhängen von Sanktionen gilt. Der neue Mechanismus behält laut dem Rat das Herkunftslandprinzip bei, wonach das Recht des Staates gilt, an dem ein Unternehmen seinen Hauptsitz in der EU hat.

Die Landesmedienanstalten hatten zuvor gewarnt der DSA drohe „ein bürokratisches Monstrum unter staatlicher Kontrolle zu kreieren". Das Prinzip der Staatsferne für die Medienaufsicht werde nicht eingehalten und bereits funktionierenden Kontrollorganen die Arbeit erschwert, da die neue Struktur in zahlreichen Fällen die exekutive Gewalt unmittelbar bei der Kommission vorsieht. Zudem bleibe unklar, welche grenzüberschreitenden Fälle künftig den umständlichen Weg über nationale Koordinatoren und den Koordinierungsausschuss aller 27 Mitgliedsstaaten gehen müssten.

Nachdem das Parlament und der Rat ihre förmliche Zustimmung erteilt haben, wird der DSA 20 Tage nach seiner Veröffentlichung im EU-Amtsblatt in Kraft treten. Die Vorschriften werden dann nach 15 Monaten – spätestens Anfang 2024 – direkt anwendbar sein. Eine nationale Umsetzung der Verordnung in den Mitgliedsstaaten ist nicht erforderlich. Damit werden hierzulande auch Teile des Netzwerkdurchsetzungsgesetzes (NetzDG) ersetzt.

Zu dem Digitalpaket der EU gehört auch der Digital Markets Act (DMA), der neue Wettbewerbsinstrumente zum Einhegen marktmächtiger Plattformen mit sich bringt. Über die Prinzipien dieser Verordnung hatten sich die EU-Gremien schon im März 2022 verständigt. Das Wettbewerbsgesetz soll verhindern, dass Konzerne wie Google und Facebook in Europa ihre Marktmacht gegenüber ihren Konkurrenten missbrauchen.

Für EU-Verhältnisse war die Verabschiedung des DSA und des DMA rasant schnell. Im Dezember 2020 waren die Entwürfe erstmals vorgestellt worden. Der von Donald Trump entfachte Sturm auf das US-Kapitol zeigte dann auf, wie gefährlich es werden kann, wenn sich Verschwörungstheorien im Netz ausbreiten. Francis Haugen machte publik, dass Facebook so einiges in Kauf nimmt, um den Profit nicht zu gefährden: Hatespeach, Gewalt, psychische Schäden bei Jugendlichen. Als glückliche Fügung erwies sich auch, dass zuletzt Frankreich die Ratspräsidentschaft innehatte. Es passte sehr gut zum Wahlkampf des wiedergewählten Präsidenten Emmanuel Macron US-Konzerne an die Kandare zu nehmen.

- Reaktionen

Kommissionspräsidentin Ursula von der Leyen (CDU) feierte die erzielte Einigung als „historisch". Pirat Breyer kritisierte dagegen: „Die Bezeichnung ‚digitales Grundgesetz' verdient das neue Regelwerk insgesamt nicht, denn der enttäuschende Deal versagt vielfach beim Schutz unserer Grundrechte im Netz." Die Privatsphäre werde weder durch ein Recht auf anonyme Internetnutzung noch durch eines auf Verschlüsselung, durch ein Verbot von Vorratsdatenspeicherung oder ein Recht zur Ablehnung von Überwachungswerbung im Browser (Do not track) geschützt. Völlig legale Berichte und Informationen könnten gelöscht werden. Die grüne MdEP Alexandra Geese beschreibt die potenziellen Auswirkungen des Gesetzes dagegen hoffnungsvoll als „Beginn eines digitalen Frühlings". Für sie handelt es sich auch um den „ersten, entscheidenden Schritt zu mehr Demokratie und Freiheit im Netz".

Ex-US-Präsidentschaftskandidatin Hilary Clinton twitterte: „Viel zu lange haben Technologieplattformen Desinformation und Extremismus verbreitet, ohne dafür zur Rechenschaft gezogen zu werden. Die EU ist jetzt bereit etwas dagegen zu tun." Sie forderte „unsere transatlantischen Verbündeten" daher auf den DSA „über die Ziellinie zu bringen und die globale Demokratie zu stärken, bevor es zu spät ist". Ähnlich hatte sich Ex-US-Präsident Barack Obama geäußert und Gesetzesanpassungen in den USA gefordert.

Der Bundesminister für Digitales, Volker Wissing (FDP), nannte die Übereinkunft einen „Meilenstein“. Bundesjustizminister Marco Buschmann (FDP) freute sich: „Nun ist der Weg frei für einheitliche Vorgaben für soziale Netzwerke und andere Online-Plattformen in Europa.“ Sie dürften Beiträge künftig nicht mehr willkürlich entfernen und müssten ihre Löschentscheidungen auf Antrag überprüfen. Morddrohungen, aggressive Beleidigungen und Aufrufe zu Gewalt hätten auf den Portalen nichts mehr zu suchen.

Sven Giegold (Grüne), Staatssekretär im Bundeswirtschaftsministerium, hob hervor, dass die EU mit der Verordnung „weltweit die schärfsten Standards für ein freies und demokratisches Internet“ schaffe. Dies sei „nicht zuletzt vor dem Hintergrund des Ukraine-Kriegs und den damit einhergehenden Desinformationskampagnen“ wichtig. Die Vorsitzende des Digitalausschusses im Bundestag, Tabea Rößner (Grüne), erklärte: „Der DSA bietet eine Sicherheitsstruktur gegen unrechtmäßige Inhalte ohne willkürlich die Meinungsfreiheit zu gefährden“. Kritisch bewertete sie die gestaffelten und komplexen neuen Aufsichtsstrukturen.

Politiker von SPD, CDU und der Linken im EU-Parlament begrüßten die Übereinkunft. Der Vorsitzende der Linksfraktion, Martin Schirdewan, wies darauf hin, dass der Kompromiss den ursprünglichen Vorschlag der EU-Kommission mit Teilverboten spionierender Werbung „deutlich“ verbessere. Dies meinte auch die für Digitales zuständige Vizepräsidentin der Brüsseler Regierungsinstitution, Margrethe Vestager, und erklärte: „Die Demokratie ist zurück.“

- Mediensektor

Das sehen Organisationen aus dem Mediensektor völlig anders. Der Deutsche Journalisten-Verband (DJV) bezeichnete den Kompromiss als „verfassungswidrig“. Der Medienverband der freien Presse (MVFP) und der Bundesverband Digitalpublisher und Zeitungsverleger (BDZV) machten die Einigung als „Gefahr für die Pressefreiheit und Meinungsvielfalt“ aus. Der DJV-Bundesvorsitzende Frank Überall bewertet die Bündelung der Zuständigkeit für die Regulierung von Online-Inhalten auf der europäischen Ebene und die Schaffung eines festen Rechtsrahmens für große internationale Anbieter wie Facebook und Google als Gefahr und befürchtet: „Auf diese Weise wird die bewährte föderale Medienordnung, wie wir sie in Deutschland haben, mit einem Federstrich abgeschafft.“

Die Medienregulierung ist hierzulande bislang vor allem Sache der Bundesländer, während der Bund selbst bereits zahlreiche Vorgaben für Inhalte im Internet wie das NetzDG geschaffen hat. DJV-Chef Überall kann zwar nachvollziehen, dass in Brüssel angesichts der russischen Propagandaaktivitäten im Netz Handlungsbedarf gesehen werde. Aber auch hier gelte: „Gut gemeint ist nicht gut gemacht.“

Gegen die Zentralisierung auf EU-Ebene sprechen aus Sicht des DJV-Vorsitzenden auch die kulturellen Unterschiede zwischen den Mitgliedstaaten. Äußerungen, die in Polen als Beleidigung oder Schmähung aufgefasst würden, könnten in Deutschland womöglich als scharfe Form freier Meinungsäußerung zulässig sein und umgekehrt: „Nach welchen Kriterien will die EU dann entscheiden?“

Ähnlich äußerten sich der MVFP (ehemals Verband Deutscher Zeitschriftenverleger) und der BDZV. Sie monieren, die EU verpflichte Plattformen nicht nur zum Löschen rechtswidriger Inhalten. Sie wolle „diesen auch erlauben rechtmäßige Veröffentlichungen zu sperren“. Damit bestehe die Gefahr, dass „Google und Facebook über Inhaltsvorgaben in ihren Nutzungsbedingungen auch legale journalistische und redaktionelle Inhalte“ blockierten. Die Gatekeeper würden so in Teilen zu Zensoren. Auch die Verlegerverbände meinten: „Die föderale Medienregulierung ist ein Garant dafür gewesen, dass in Deutschland eine der vielfältigsten Medienlandschaften der Welt besteht. Dies darf durch europäische Vorgaben und Regulierungsbehörden nicht gefährdet werden.“

Der Rechts- und der Kulturausschuss des Parlaments hatten zuvor vergeblich auf eine „Medienausnahme“ gedrängt, wonach Betreiber sozialer Netzwerke journalistische Inhalte nicht hätten löschen dürfen. Gegner sahen in dieser Klausel ein Einfallstor für Desinformation. Die allgemeine Bestimmung zum Schutz der Grundrechte im DSA und der Verweis auf das in der EU anwendbare Medienrecht reichen dem MVFP und dem BDZV nicht.

- Wirtschaftsverbände

Die auf EU-Ebene gefundene Übereinkunft beim Digital Services Act (DSA) hat zugleich viele Unterstützer. Der Bundesverband Digitale Wirtschaft (BVDW) begrüßte das Gesetz für digitale Dienste prinzipiell als überfällig. Der Kampf gegen illegale Inhalte und „Hate Speech“ im Netz sowie der Schutz der Nutzer sei heute wichtiger denn je. Es bestehe aber auch „die Gefahr für erhebliche Einschränkungen und Rechtsunsicherheiten für Unternehmen“ vor allem im Umgang mit Design-Tricks wie „Dark Patterns“. Sollten die Restriktionen hier für alle Firmen im Anwendungsbereichs des DSA gelten, „würde das der digitalen Wirtschaft massiv schaden“.

Als zeitgemäß und zukunftsfähig bezeichnet der BVDW den Kompromiss beim Kinder- und Jugendschutz. Ein Verbot gezielter „datenbasierter Werbung“ gelte bei Minderjährigen wohl nur, „wenn die Betreiber von Online-Plattformen positive Kenntnis davon haben“, dass die Nutzung des Angebots durch eine Person unter 18 Jahren erfolgt. Unternehmen stünden damit nicht vor der Herausforderung selbst einschätzen zu müssen, „wer vor dem Endgerät sitzt“.

Selbst den Bann der Verarbeitung sensibler Daten bei personalisierter Werbung hält der Verband für richtig, zumal ein solcher bereits in der Datenschutz-Grundverordnung (DSGVO) angelegt sei. Der IT-Verband Bitkom kann mit der Einigung an diesem Punkt ebenfalls leben: Er begrüßt, „dass personalisierte Werbung in sozialen Netzwerken weiterhin ermöglicht wird“. Wichtig sei, dass der Rechtsrahmen auch in der Praxis funktioniere und gleichzeitig der Plattformökonomie „Entfaltungsspielraum für Innovationen lässt“.

- Verbraucher- und Bürgerrechtsorganisationen

Insgesamt sei der DSA eine gute Nachricht für die Konsumenten, heißt



Bild: iStock.com/ peepo

es beim BEUC, dem Dachverein der europäischen Verbraucherschutzorganisationen. Neue Pflichten für Plattformen, die Legitimität ihrer Geschäftskunden zu überprüfen, Transparenzanforderungen und Optionen für Nutzer, den Grad der Personalisierung von Empfehlungssystemen zu wählen, seien genauso begrüßenswert wie die Gewährleistung wirksamer Rechtsmittel. Bedauerlich sei, dass das Gesetz „nicht die gesamte Bandbreite an Maßnahmen zur Bekämpfung illegaler Aktivitäten auf Online-Marktplätzen enthält". Es fehlten Haftungs- und Schadenersatzpflichten, wenn Kunden etwa ein „unsicheres Produkt" angedreht bekämen.

Für Amnesty International stellt der DSA „einen Wendepunkt in der Geschichte der Internetregulierung dar". Big-Tech-Plattformen wie Facebook und Instagram sowie YouTube müssten damit erstmals „systemische Risiken" ihrer Dienste wie die Befürwortung von Hass und die Verbreitung von Desinformation bewerten und bewältigen sowie die Blackbox ihrer Algorithmen öffnen. Die Gesetzgeber hätten aber die Chance verpasst „alle invasiven, auf Überwachung basierenden Werbepraktiken" abzuschaffen, „um die Rechte der Menschen auf Privatsphäre, Datenschutz und Nichtdiskriminierung wirklich zu wahren". Der Erfolg hänge nun von einer „rigorosen" Durchsetzung ab.

Die Bürgerrechtsorganisation European Digital Rights (EDRi) äußerte sich ähnlich und sprach von einem „ersten Schritt in die richtige Richtung". Etwa beim Vorgehen gegen Dark Patterns wäre mehr drin gewesen.

- Wissenschaft

Schon im Sommer 2021 bei der Vorlage des Entwurfes hatte die US-Wirtschaftswissenschaftlerin Shoshana Zuboff, die den Begriff des „Überwachungskapitalismus" prägte, geschrieben: „Freunde, schaut alle auf das Europaparlament." Der Stuttgarter Medienrechtler Tobias Kerber bewertet das Paket aus DSA und DMA als „einen neuen globalen Standard zur Regulierung der Digitalwirtschaft": „Die als Verordnung konzipierten und daher unmittelbar anwendbaren Vorgaben stellen das rechtliche Betriebssystem für digitale Dienste auf eine gänzlich neue Version um." Kerber lobt, dass Facebook, Google, Amazon & Co. mit dem DSA die „Vorgänge in ihren Maschinenräumen" transparenter und nachvollziehbarer gestalten müssten. Zudem werde mit den Schranken für Dark Patterns „neben dem insoweit defizitär aufgestellten Datenschutzrecht" jetzt eine Regel etabliert, die es den großen Unternehmen zumindest schwerer machen solle Nutzer zu übervorteilen.

Als „hochbrisant" schätzt der Professor dagegen den auf den letzten Metern eingefügten Mechanismus zur Reaktion auf Krisen ein. Dieser werde es unter Umständen erlauben im Falle eines Notstands „erhebliche Eingriffe in die Meinungs- und Informationsfreiheit zuzulassen". So dürften etwa als Desinformation oder Propaganda bewertete Inhalte von Plattformen – wie aktuell im umstrittenen Fall RT und Sputnik – nicht weiterverbreitet werden. Völkerrechtlich müssten Staaten Kriegspropaganda zwar unterbinden. Medienrechtlich sei in Europa aber eigentlich ein freier Informationsfluss vorgesehen.

Auch Matthias Kettemann, der in Hamburg und Innsbruck Medientheorie erforscht und lehrt, bewertet den DSA als „bedeutsamen neuen Rechtsakt". Das Gesetz werde „in vielen Bereichen der Internetkommunikation für mehr Fairness, Rechtssicherheit und Rechenschaftspflicht" sorgen. Gerade für deutsche Nutzer, die schon Erfahrungen mit dem Netzwerkdurchsetzungsgesetz hätten, handle es sich aber um „keine Revolution". Neu sei, dass Plattformen besser moderieren, ihre Regeln klarer gestalten und „professioneller mit Beschwerden umgehen" müssten.

Verwendete Quellen: Kelnberger, Anleitung zur Gegenrevolution, SZ 17.01.2022, 6; Krempl, Digital Services Act: EU-Gremien einigen sich auf „Plattform-Grundgesetz", www.heise.de 23.04.2022, Kurzlink: https://heise.de/-7063141; Krempl, Digital Services Act: Upgrade fürs rechtliche Betriebssystem von Facebook & Co., www.heise.de 24.04.2022, Kurzlink: https://heise.de/-7063485; Krempl, Digital Services Act: Wie die EU das Internet künftig regulieren wird, www.heise.de 24.04.2022, Kurzlink: https://heise.de/-7063328; Krempl, Digital Services Act: Medienverbände nennen Plattformgesetz „verfassungswidrig", www.heise.de 25.04.2022, Kurzlink: https://heise.de/-7064548; Kelnberger, Neue Regeln fürs Netz, SZ 25.04.2022, 15.

Heinz Alenfelder

Neues aus der „Hauptstadt des Datenschutzes“: BigBrotherAwards 2022

Die Verleihung der deutschen BigBrotherAwards (BBA) fand auch 2022 wieder im Rahmen eines Festakts Ende April in Bielefeld, der „Hauptstadt des Datenschutzes“, statt. Wie schon die Jahre zuvor wurden Preise in verschiedenen Kategorien sowie für das Lebenswerk verliehen und in Laudationes begründet. Dieser Bericht beleuchtet kurz die Hintergründe der „Oscars für Datenkraken“, gibt einen Überblick über die ausgezeichneten Gewinner und wird ergänzt um einige Eindrücke von der Gala.

Der Verein Digitalcourage übernahm im Jahr 2000 (damals noch als FoeBuD) die Idee der BigBrotherAwards aus Großbritannien. Die englische Bezeichnung für diesen Datenschutz-Negativpreis blieb zwecks Wiedererkennung erhalten. In Zusammenarbeit mit anderen Bürgerrechtsorganisationen wurde eine Jury zusammengestellt, die die in jedem Jahr zahlreich eingehenden Meldungen über Preisverdächtige sichtet, bewertet und in mühevoller Kleinarbeit nachrecherchiert. Während der ersten zehn Jahre druckte die DANA alle Laudationes und oft auch darüber hinausgehendes Material im Umfang von zehn bis zwanzig Seiten ab. Später, als die BBA sich etabliert hatten, verwies meist ein deutlich kürzerer Bericht auf die Webseite, die unter bigbrotherawards.de ein vielfältiges Informationsangebot bereit hält. Nicht nur die Preisträger aus allen Jahren werden dort aufgelistet, sondern als interessante Ergänzung kann in der Rubrik „Updates“ seit 2017 verfolgt werden, wie die als Datenkrake Ausgezeichneten auf die Auszeichnung reagiert haben. Oft – so das Organisationsteam – wird übrigens vor der Verleihung mit rechtlichen Konsequenzen gedroht, die jedoch bisher immer unterblieben sind. padeluun, neben Rena Tangens einer der Hauptinitiatoren, betonte vorab im Pressegespräch, dass sich die BBA-Jury nicht als rechtliche Institution sieht, die nur Illegales aufdecken will, sondern immer auch den Austausch mit den Preisträgern sucht. Zu diesem Zweck werden vor der Preisverleihung sowohl die Geschäftsführung als auch die Datenschutzbeauftragten und die jeweilige Presseabteilung der betroffenen Firmen, Behörden und Institutionen informiert und zur Gala eingeladen. Erschienen ist während der Veranstaltung – wie in den meisten Vorjahren – niemand.

Von der Jury (siehe Kasten) wurden im Jahr 2022 in den Kategorien Technik, Behörden und Verwaltung, Arbeitswelt, Verbraucherschutz und auch für ein Lebenswerk die folgenden Preise vergeben:

- Die Bundesdruckerei GmbH erhielt den Technik-BBA, da sie in einem Projekt mithilfe (und zur Beförderung) der Blockchain-Technik digitale Schulzeugnisse erstellen will. Laudator Frank Rosengart: „Viele Anwendungen für digitale Echtheitsprüfungen lassen sich besser mit klassischen, ‚von oben nach unten‘-Zertifikaten lösen. … Die große Gefahr in der Blockchain liegt darin, dass alle Eintragungen lückenlos nachvollziehbar sind.“
- Der Behörden-BBA 2022 ging an die deutsche Polizei, vertreten durch das Bundeskriminalamt, das entgegen der verfassungs- und europarechtlichen Vorgaben personenbezogene Daten in Dateien nicht oder unzureichend kennzeichnet, so dass für Millionen Menschen die Gefahr besteht von der Polizei oder anderen Behörden ungerechtfertigter Weise als Gefährder oder Straftäter behandelt zu werden. Auch im Projekt „Polizei 2020“, einem gemeinsamen „Datenhaus“ von Bund und Ländern, scheint sich dies nicht wesentlich zu ändern, zumal die vielkritisierte amerikanische Firma Palantir in Bayern den Zuschlag bekommen hat. Die Laudatio hielt Thilo Weichert und er betonte darin: „Der BigBrotherAward in der Kategorie Verwaltung geht aber vorrangig nicht an das Bayerische LKA, sondern an das BKA … das die Gesamtverantwortung für ‚Polizei 2020‘ trägt“.
- Der BigBrotherAward in der Kategorie Arbeitsrecht wurde Lieferando und den deutschen Betreibern des Angebots, yd.yourdelivery GmbH und Takeway Express GmbH, zugesprochen, weil in diesem Unternehmen eine unzulässige Totalkontrolle aller beschäftigten „Rider“ mit Hilfe der Scoober-App erfolgt, die detailliert und sekundengenau eine Fülle von Verhaltensdaten erfasst. In der Laudatio betonte Peter Wedde: „Das Bundesarbeitsgericht sieht in dauerhaften Überwachungsmaßnahmen von Beschäftigten (im Regelfall) einen unzulässigen Eingriff in die Persönlichkeitsrechte.“
- Zur Verleihung des BBA in der Kategorie Verbraucherschutz fasste der Laudator padeluun zusammen: „Klarna … hat ein unklares Geschäftsmodell, droht Kundinnen und Kunden mit überhöhten Mahngebühren und greift tief in die Trickkiste, um sich deren Privatsphäre zu bemächtigen.“ Das schwedische Unternehmen Klarna Bank AB erhielt den BBA wegen der Bündelung von Daten und Macht als Shopping-Service, Zahlungsdienstleister, Preisvergleichsportal, persönlicher Finanzmanager, Bonitätskontrolleur und Bank.
- Schließlich begründete Rena Tangens die Vergabe des BBA für das Lebenswerk an die Irische Datenschutzaufsichtsbehörde (DPC), vertreten durch Helen Dixon. Deren dauerhafte Sabotage von Bemühungen europäisches Datenschutzrecht durchzusetzen führt dazu, dass sich Irland für die großen Player des Internets zu einem reinen Daten-El-Dorado entwickelt hat. Mit verschiedenen „Tricks“ umgeht die Irische Datenschutzaufsicht die Bearbeitung von Beschwerden.

Rena Tangens: „Es fehlt schlicht am europäischen Geist“. Den Wortlaut ihres Beitrags finden Sie gleich im Anschluss an diesen Artikel. Das Publikum entschied zum Schluss der Laudationes, dass dies der Hauptgewinner des Jahres 2022 ist.

Die diesjährige Gala zur Verleihung der BBA fand wieder im hybriden Format statt. Mit großem Engagement hatten über 70 Angestellte und Ehrenamtliche von Digitalcourage Vorbereitungen getroffen, die eine gelungene Veranstaltung mit ansprechenden Bühnenbildern in einer angenehmen Atmosphäre in der Bielefelder Hechelei möglich machten. Neben der musikalischen Untermalung durch das Kristin Shey Jazz Quartett sorgte der durch das Programm führende Moderator Andreas Liebold für eine aufgelockerte Stimmung, indem er einige Quizfragen stellte und auch mal Werbung für Spenden an Digitalcourage einflocht. Peter Weddes Laudatio für Lieferando wurde per Video eingespielt und ebenso grüßte der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Ulrich Kelber, per Videoaufzeichnung. Mit einem Umtrunk schien die Veranstaltung beendet, hätte sich nicht im Laufe des Abends noch der Betriebsratsvorsitzende von Lieferando eingefunden, um den Preis dankend entgegen zu nehmen. Er versteht ihn laut der Nachricht von Digitalcourage auf dem Nachrichtendienst Mastodon „als Unterstützung für die Rechte der Fahrer.innen“.

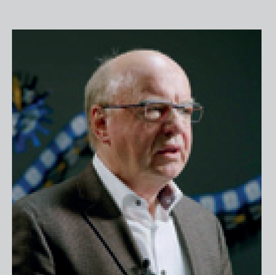
Die Jury der BigBrotherAwards 2022



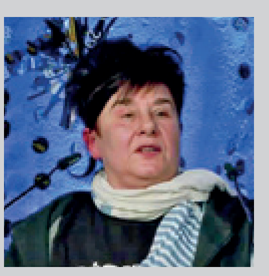
Frank Rosengart
Chaos Computer Club, programmiert im Kommunikationsbereich. Der Chaos Computer Club e.V. (CCC), 1981 gegründet, ist die größte europäische Hackervereinigung.



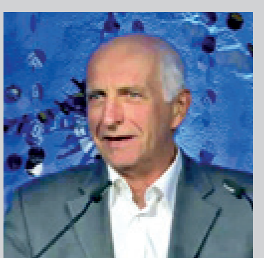
padeluun
Digitalcourage, ist Künstler und Gründungsvorstand von Digitalcourage. Digitalcourage setzt sich seit 1987 für eine lebenswerte Welt im digitalen Zeitalter ein und veranstaltet seit 2000 die BigBrotherAwards in Bielefeld.



Prof. Dr. Peter Wedde
Frankfurt University of Applied Sciences, ist Professor für Arbeitsrecht und Recht der Informationsgesellschaft sowie Herausgeber und Autor.



Rena Tangens
Digitalcourage, ist Künstlerin, Internet-Pionierin und Vorstand von Digitalcourage. Sie hat 1987 Digitalcourage – damals als FoeBuD – mitgegründet. Für ihre Arbeit wurde sie bereits mehrfach ausgezeichnet



Dr. Thilo Weichert
Deutsche Vereinigung für Datenschutz und Netzwerk Datenschutzexpertise, ist ehemaliger Datenschutzbeauftragter des Landes Schleswig-Holstein. Das Netzwerk Datenschutzexpertise ist ein Zusammenschluss von Experten und Expertinnen, die Gesetze und Technologien juristisch und technisch detailliert analysieren.

Die Bilder wurden aus dem BBA-Video 2022 entnommen:
https://digitalcourage.video/w/1JGytG6mwhNdbxX1UJjUv8

Laudatio zum BigBrotherAward 2022 in der Kategorie „Lebenswerk“: Die Irische Datenschutzbehörde (DPC – Data Protection Commissioner)

Ein BigBrotherAward 2022 geht an die irische Datenschutzaufsicht, kurz DPC (Data Protection Commission), vertreten durch ihre Chefin Helen Dixon, für ihre umfassende Sabotage des europäischen Datenschutzrechts. Und weil die irische Datenschutzaufsicht das so planvoll, seit so vielen Jahren und mit solch kafkaesker Phantasie betreibt, reicht dafür die Kategorie „Behörden und Verwaltung“ nicht aus. Dafür gibt es den Preis fürs Lebenswerk.

Die irische Datenschutzaufsicht verhindert, dass geltendes Recht durchgesetzt wird – durch jahrelanges Verschleppen, de facto Nicht-Bearbeiten von Beschwerden, bürokratische Winkelzüge, abschreckende Kosten für Beschwerdeführer und mangelnde Kooperation mit den europäischen Kolleginnen und Kollegen. Behördenchefin Helen Dixon agiert erratisch und reagiert allergisch auf Kritik. Ihre Behörde lässt das europäische Datenschutzrecht ins Leere laufen – und das ausgerechnet gegenüber denen, die harte Kontrolle nötig hätten: Google, Facebook, Apple, Microsoft & Co.



Laudatorin Rena Tangens

Arbeitsverweigerung

Die Arbeitsverweigerung der irischen Datenschutzaufsicht betrifft dabei nicht nur Menschen, die in Irland leben, sondern sie gefährdet die Persönlichkeitsrechte von 450 Millionen EU-Bürgerinnen und Bürgern.

Rückblende: Mai 2018 – die europäische Datenschutzgrundverordnung tritt in Kraft. Sie stellt klar: 1. Egal, aus welchem Land ein Unternehmen kommt – sobald es persönliche Daten von EU-Bürger.innen verarbeitet, muss es sich an die in der EU geltenden Datenschutzregeln halten. Das ist das „Marktortprinzip“. 2. Bei Datenschutzvergehen drohen nun endlich empfindliche Bußgelder. „Empfindlich“ heißt: bis zu 4 % des weltweit erzielten Jahresumsatzes. Damit wurde Datenschutz bei den Konzernen zur Chefsache. Yay!

Doch leider haben wir uns zu früh gefreut: Denn ein europäisches Gesetz zu machen reicht nicht – seine Einhaltung muss auch in allen EU-Staaten durchgesetzt werden. Und da gibt es ein Problem. Es heißt: Irland.

Weshalb?

Jedes Unternehmen muss eine federführende Datenschutzaufsichtsbehörde festlegen, und zwar in dem Land, in dem das Unternehmen seine Hauptniederlassung in der EU hat. Diese federführende Aufsichtsbehörde ist fürderhin die Hauptansprechadresse für alle Beschwerden gegen dieses Unternehmen. Wenn sich Bürger.innen oder Organisationen über die Datenverarbeitung einer Firma beschweren wollen, tun sie das bei der Datenschutzaufsicht in ihrem eigenen Land. Diese leitet die Beschwerde dann an die zuständige Datenschutzaufsicht am Hauptsitz des beklagten Unternehmens weiter. Die Regelung, dass die Datenschutzaufsicht eines Unternehmens jeweils in den Händen nur eines EU-Landes liegt, heißt „One-Stop-Shop“.

Das klingt erst einmal praktisch – da wird Kompetenz gebündelt und die Aufsichtsbehörde kennt ihre Pappenheimer vor Ort und muss sich nicht bei jeder Beschwerde neu einarbeiten.

Doch es gibt einen Haken: Die großen Digitalkonzerne mit ihren immateriellen Geschäften können ihren „Hauptsitz“ relativ flexibel handhaben. Entsprechend suchen sie sich eine ihnen genehme Datenschutzaufsicht und eröffnen dann dort ihren vorgeblichen Hauptsitz.

Hier fällt eine gewissen Ballung ins Auge – Irland: Home of Google, Apple, Facebook und WhatsApp, Microsoft und LinkedIn, Adobe, Tiktok, Airbnb, Tinder, Twitter, Dropbox, Yahoo und so weiter.

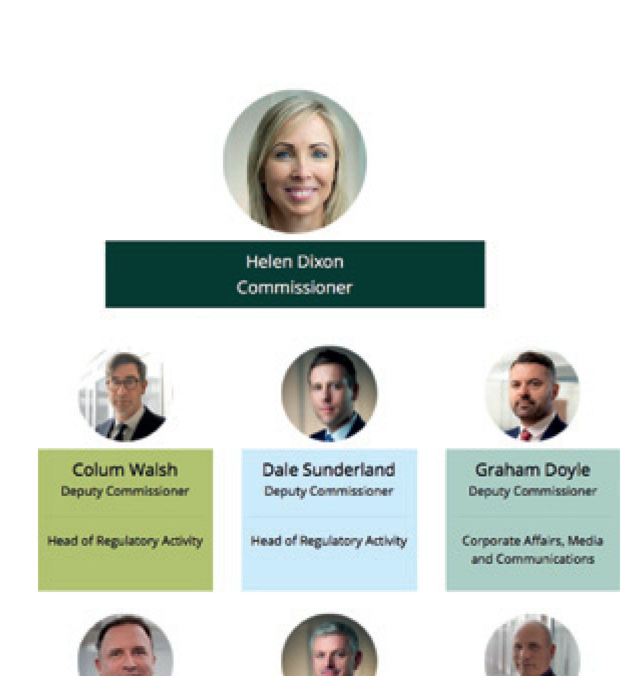
Tja, was könnte wohl die Ortswahl der Digitalkonzerne beeinflussen?

Das grüne Gras, die weiten Wiesen, das dunkle Bier, ... oder liegt es ganz vielleicht doch an den Eigenheiten der Datenschutzaufsicht in Irland?

Schauen wir uns das mal genauer an:

Welche Bedeutung Irland dem Datenschutz gibt, das dokumentiert eindrucksvoll das Dienstgebäude der irischen Datenschutzaufsicht: Ein Büro im ersten Stock über einem kleinen Supermarkt in der Kleinstadt Portarlington – mehr als 70 Kilometer südwestlich von Dublin, jott we de. Das Foto der Datenschutzbehörde mit Supermarkt belustigt seit vielen Jahren die Presse in ganz Europa. Ja, inzwischen ist der Centra Supermarkt einem Spar gewichen und es ist immerhin einmal neu gestrichen worden.

2017 wurde ein zusätzlicher Behördensitz ganz repräsentativ mitten in der Hauptstadt Dublin eröffnet. Keineswegs aber, um der gestiegenen Bedeutung des Datenschutzes in Europa gerecht zu werden, sondern – Zitat eines Sprechers der Behörde – „um besseren Kontakt zu den multi-nationalen Unternehmen zu halten, die sich in Dublin angesiedelt haben“(!).[1]



Kreative Behörde

Die irische Datenschutzaufsicht gibt sich jede erdenkliche Mühe das von Big Tech in sie gesetzte Vertrauen nicht zu enttäuschen. Und dafür lassen sie sich ganz schön viel einfallen:

Wichtigste Taktik: Beschwerden gegen die großen Digitalkonzerne einfach liegen lassen.

Fälle schlicht nicht bearbeiten.

Ein paar Zahlen zur Illustration: Seit Geltungsbeginn der DSGVO im Mai 2018 hat Ulrich Kelber, der deutsche Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), etwa 50 Verfahren zuständigkeitshalber an die irische Datenschutzaufsicht abgegeben – überwiegend Verfahren gegen WhatsApp. Von diesen 50 Verfahren ist nicht eines durch eine inhaltliche Entscheidung abgeschlossen worden.

Laut Gesetz müssen Beschwerden „unverzüglich“ bearbeitet werden. Die irische Datenschutzaufsicht argumentiert gerade vor dem irischen High Court, dass vier Jahre Bearbeitungszeit immer noch „unverzüglich“ seien …

Den enormen Rückstau bei der Bearbeitung der Beschwerden erklärt die irische Datenschutzaufsicht damit, dass sie zu wenig Geld und zu wenig Personal hätte.

Doch die Behörden großer Mitgliedsstaaten wie Spanien oder Frankreich verfügen über ähnliche Budgets wie das kleine Irland. Die spanische Datenschutzaufsicht hat etwa das gleiche Budget und haut mehrere Entscheidungen pro Tag raus – die Iren schaffen nur ein paar pro Jahr. Es liegt also nicht am Geld, sondern an der Effizienz. Die Mitarbeiterzahl ist in Irland inzwischen von rund 30 (im Jahr 2014) auf 195 (im Jahr 2021) aufgestockt worden – leider ohne dass das die Arbeitsergebnisse verbessert hätte. Die Aufsichtsbehörden anderer Länder, u.a. Deutschland, haben den irischen Kolleg.innen schon vor Jahren Hilfe bei der Bearbeitung der Fälle angeboten. Doch Helen Dixon hat alle Hilfsangebote ausgeschlagen.

Zweite Taktik: Statistik-Bullshit verbreiten.

Viel Energie der Behörde wird offenbar in Public Relations und hübsch gestaltete Tätigkeitsberichte gesteckt, um das Nichtstun gut aussehen zu lassen. Im Tätigkeitsbericht vom März 2022 steht, dass 626 von 969 grenzüberschreitenden Beschwerden, die seit Mai 2018 eingegangen seien, abgeschlossen wurden. Aber Moment mal: Was bedeutet „abgeschlossen“? Offenbar nicht, dass die Fälle bearbeitet und entschieden wurden.

Ein weiterer Fall von Zahlen-Kosmetik: Zuvor hatte die irische Datenschutzaufsicht rund 10.000 „cases“ (Fälle) pro Jahr auf dem Tisch Doch im Tätigkeitsbericht 2021 gibt es plötzlich nur noch rund 3.400 „complaints“ (Beschwerden), dazu aber rund 7.500 „inquiries“ (Anfragen). Der Trick: Alles, was bei der Einreichung nicht explizit „Beschwerde“ genannt wurde, fällt unter „Anfragen“. Anfragen landen im Papierkorb. Auch das ist natürlich eine Art „sich damit befassen“ und „abzuschließen“: Ablage P. Erledigung durch Umbenennung.

Taktik Nummer drei: Ausschluss der Beschwerdeführer.innen vom Verfahren.

Dafür gibt es eine ganze Reihe von Tricks, zum Beispiel:

a) Die Erpressungs-Methode:

Die Behörde fordert vom Kläger die Unterzeichnung einer Verschwiegenheitserklärung (englisch „Non Disclosure Agreement“, kurz NDA). Das heißt, er müsste Stillschweigen über die Verhandlung, die Verhandlungsergebnisse und die dort vorgelegten Informationen wahren. So geschehen mit Johnny Ryan vom Irish Council for Civil Liberties bei seiner Klage gegen Googles Real Time Bidding Werbeauktionen. So geschehen mit Max Schrems von noyb („none of your business“) bei seiner Klage gegen Facebook. Damit will die irische Datenschutzaufsicht dafür sorgen, dass alles hübsch intern und unterm Deckel gehalten wird. So etwas kann eine klagende Verbraucher- und Bürgerrechtsorganisation einfach nicht unterschreiben! Nach Nichtunterzeichnung wurde Max Schrems von seinem eigenen Verfahren ausgeschlossen. Was allen EU-Grundrechten widerspricht.

b) Die Umgehungsmethode:

Die irische Behörde leitet ein paralleles „amtsseitiges Verfahren“ zum selben Thema wie eine Beschwerde ein. Fortan wird nur noch dieses amtsseitige Verfahren bearbeitet – und solange lässt sie das Verfahren des Beschwerdeführers ruhen. Nach der Entscheidung des amtsseitigen Verfahrens wird dann das andere beendet, denn das Thema ist ja jetzt erledigt! Chapeau – eine wirklich elegante Art, die Bürger.innen von ihren eigenen Verfahren auszuschließen.

c) Die „Klag-doch-wenn-du-es-dir-leisten-kannst“-Methode:

Bei Untätigkeit der irischen Datenschutzbehörde den Rechtsweg einzuschlagen und zu klagen ist eine so teure Angelegenheit, dass sie für Privatleute quasi nicht in Frage kommt. Dazu trägt u.a. die irische Regel bei, dass jedes Gesetz, auf das man sich bezieht, nicht

nur als „nach Paragraph xy“ benannt werden, sondern vor Gericht vorgelesen werden muss. Das dauert nicht nur lang - sondern wird bei den bis zu 1000 Euro, die Anwaltskanzleien pro Stunde kassieren, auch sehr, sehr teuer für die Klagenden. Ein Beispiel: Im „Privacy Shield“-Fall („Schrems II“) ging es um die Datenübermittlung von Facebook in die USA. Bei dem Fall gab es drei Parteien (Facebook, die Irische Datenschutzaufsicht und Max Schrems). Wer verliert, muss die Kosten von allen drei Parteien zahlen – die beliefen sich in diesem Fall auf insgesamt rund 10 Millionen Euro (!). Was für ein Glück, dass Max Schrems gewonnen und die Datenschutzbehörde verloren hat.

Soviel zur Kreativität der irischen Behörde – nun zu den Kopfnoten:

Mangelnde Kollegialität, kein europäischer Geist, Geheimniskrämerei:

Zu all dem passt, wie Behördenchefin Dixon agiert. Sie nimmt an fast keiner gemeinsamen Sitzung der europäischen Datenschutzbeauftragten teil. Sie schickt meist einen Stellvertreter, der dann aber nichts sagen kann oder darf. Die Kommunikation auf der Leitungsebene ist damit schon mal tot. Das setzt sich auf der Sachbearbeitungsebene fort: Anfragen per E-Mail von deutschen oder österreichischen Kolleg.innen werden oft nicht beantwortet, Telefonanrufe nicht angenommen. Mitarbeiter.innen von anderen Datenschutzbehörden werden von den Iren gern „geghostet“, also komplett ignoriert, Akten nicht an die europäischen Kolleg.innen übermittelt. Die irische Behörde wirkt wie ein „schwarzes Loch“, in dem alles verschwindet.

Ihre Arbeitsverweigerung hat aber eben nicht nur für Menschen in Irland Folgen, sondern für 450 Millionen Menschen in der EU, deren Rechte von den großen Digitalkonzernen mit Füßen getreten werden. Das Gebaren der irischen Datenschutzaufsicht führt dazu, dass europaweit kleine und mittelständische Firmen bei Datenschutzvergehen von ihrer nationalen Aufsichtsbehörde sanktioniert werden; die großen Digitalkonzerne aber zeigen uns allen eine lange Nase: „Ätsch – beschwert euch doch – wir sind in Irland.“

Nun fragen wir uns: Warum tun die das?!

Durch all diese Winkelzüge und miesen Tricks macht die irische Datenschutzbehörde Irland zum Datenschutz-Freihafen, zum Schlupfloch für Verbrecher, zum Reservat für Datenkraken. All das fügt sich bestens in einen anderen Teil des inselgrünen Ökosystems ein:

Die Steueroase

Sie denken bei Steueroasen an die Cayman Inseln oder die Bahamas? Lenken Sie lieber Ihren Blick auf Irland. Offiziell gelten in Irland 12,5 % Unternehmenssteuern. Doch Irland hat es einigen ausländischen Konzernen ermöglicht die effektiven Unternehmenssteuern für ihre globalen Gewinne auf 0 bis 2,5 % zu drücken. Die Steuertricks haben so phantasievolle Namen wie „Double Irish“, „Double Irish with a Dutch sandwich“ oder „Single Malt“. Über Irlands Steuersparmodelle werden mehr Gelder der Steuer (und damit der Allgemeinheit) entzogen, als in der gesamten Karibik.[2]

Gesetzlosigkeit als Geschäftsprinzip?

Für Irland sind das lukrative Geschäfte. Es profitiert davon, dass es den Big Tech Konzernen ermöglicht ihren Überwachungskapitalismus ohne Rücksicht auf Bürgerrechte durchzuziehen. Also persönliche Daten zu sammeln, zu Profilen zu verknüpfen, Kategorien zu bilden, Menschen zu manipulieren und ihnen durch den Verkauf von Prognosen viel Handlungsfreiheit für die Zukunft zu nehmen. Irland lebt von den Brosamen von Big Tech. Und es lebt gut davon, denn auch nur 2,5 % des globalen Umsatzes von Apple ist schon eine verdammt große Menge Geld.

Wir alle zahlen dafür mit unserer Freiheit.

Doch dieses Geschäftsgebaren hat eine Kehrseite: Irland ist extrem abhängig von den Tech-Konzernen. Ein paar Zahlen:

- 2016–17 haben ausländische Firmen 80 % der irischen Unternehmenssteuern gezahlt.
- 25 der Top-50-Unternehmen in Irland sind US-kontrolliert.
- 2018 machte Apple alleine ein Fünftel des irischen Bruttoinlandsproduktes aus.[3]

Ein Abgeordneter des irischen Parlaments, der 2017 auf das schändliche Treiben der Konzerne mit dem Steuervermeidungsmodell „Single Malt“ hinwies, bekam vom irischen Finanzminister den guten Rat „to put on the green jersey“ (das grüne Trikot anziehen) – mit anderen Worten: Zum Wohle Irlands die Klappe halten.[4] Der Finanzminister machte sich also keine Sorgen wegen des Steuerbetrugs, sondern mehr wegen Irlands Reputation.

2023 kommt die globale Mindeststeuer von 15 % – und eine Digitalsteuer. Werden die Digitalkonzerne Irland verlassen, wenn der Steuervorteil versiegt ist? Oder reicht es ihnen, wenn auf der grünen Insel die Durchsetzung des Datenschutzes blockiert wird? Darauf hofft offenbar der irische Premierminister Micheál Martin. Er lobte im Februar 2022 ausdrücklich „Ms. Dixons Kompetenz und Fähigkeiten“ und forderte, dass Irland die Arbeit ihrer Datenschutzbehörde „robuster gegen Kritik verteidigen“ solle.[5]

Wie lange wollen wir das noch zulassen?

Leider ist das grüne Trikot offenbar auch bei denen beliebt, die die Einhaltung der europäischen Gesetze durchsetzen sollen. Es wäre nämlich die Aufgabe der Europäischen Kommission – genau gesagt: der Generaldirektion Justiz und Verbraucher – die irische Datenschutzaufsicht wirksam auf Vollzug des europäischen Datenschutzrechts zu kontrollieren. Tut sie aber leider seit Jahren nicht. Team Irland. Seriously?

Doch Obacht: Allmählich braut sich etwas zusammen in Europa. Denn irgendwann reicht es auch hier den diplomatischsten, freundlichsten und geduldigsten Datenschützer.innen und Politiker.innen.

Im Januar 2021 beantragt der LIBE-Ausschuss des Europäischen Parlaments (das ist der Ausschuss für bürgerliche Freiheiten, Justiz und Inneres) ein EU-Vertragsverletzungsverfahren gegen Irland einzuleiten, weil Irland die europäische Datenschutzgrundverordnung nicht ordnungsgemäß durchsetzt.[6]

Auftritt Helen Dixon: Sie fordert, dass sie dazu im LIBE-Ausschuss angehört wird. Der LIBE-Ausschuss setzt tatsächlich eine Anhörung für den 17.

März 2021 an. Nun will Dixon sogar das Verfahren vor dem europäischen Parlament bestimmen – und nicht kommen, wenn auch Kritiker wie Max Schrems geladen werden. Damit allerdings blitzt sie bei den EU-Parlamentariern ab – der Ausschuss für bürgerliche Freiheiten lässt sich das Procedere seiner Anhörungen nicht diktieren. Daraufhin erscheint Helen Dixon nicht zu der Anhörung, die sie selbst verlangt hat. Großes Kino.

Kein Wunder, dass selbst in Irland manche mittlerweile Rot sehen. Wie der Justizausschuss des irischen Parlaments, der im Juli 2021 eine grundlegende Reform der irischen Datenschutzaufsicht gefordert hat. Wobei auch dieser Schritt zur Einsicht wohl nicht passiert wäre ohne die Initiative und das Engagement von Bürgerrechtsorganisationen, die unsere Rechte gegenüber den Digitalkonzernen durchzusetzen versuchen. Unser Dank gilt beharrlichen Menschen wie Max Schrems von noyb und Johnny Ryan vom Irish Council for Civil Liberties (ICCL).

Im März 2022 hat der High Court, der höchste Gerichtshof in Irland, die Klage des ICCL gegen die irische Datenschutzaufsicht wegen Untätigkeit zugelassen. Dixons Behörde hatte die Beschwerde des ICCL wegen Googles Werbeauktionen – das sogenannte Real Time Bidding – vier Jahre lang nicht bearbeitet. Stichwort: „unverzügliche Erledigung“... Zum Thema Googles Real Time Bidding empfehle ich meine Laudatio zum BigBrotherAwards für Google von 2021. :)

Das ICCL hat außerdem die EU-Kommission aufgefordert ein Vertragsverletzungsverfahren einzuleiten. Im Februar 2022 reicht EU-Ombudsfrau Emily O'Reilly die Beschwerde wegen Untätigkeit der irischen Datenschutzbehörde an Ursula von der Leyen weiter und fordert Antwort bis 15. Mai 2022. Ausgang offen.

Was ist zu tun?

1. Das One-Stop-Shop-System ist offenbar dysfunktional und sollte grundlegend reformiert werden.[7] Wenn ein einzelnes Land aus Eigennutz die Durchsetzung der Datenschutzgrundverordnung blockieren kann, dann ist das ein struktureller Fehler.
2. Sidestepping: Datenschutzbeschwerden einfach nicht mehr nach Irland weitergeben, sondern sich selbst für zuständig erklären und entscheiden. Einige EU-Länder, z.B. Frankreich, praktizieren das bereits hier und da. Betroffene werden auch zu Gerichten gehen statt zu Datenschutzbehören, auch wenn das viel kosten kann.
3. Ein einheitliches europäisches Verfahrensrecht für grenzüberschreitende Datenschutzfälle einführen, das Fristen für die Bearbeitung und so weiter verbindlich festlegt.
4. Oder eine kompetente europäische Institution bestimmen, die die großen grenzüberschreitenden Fälle entscheidet. Das könnte zum Beispiel der Europäische Datenschutzausschuss (EDSA)[8] sein, in dem die Datenschützer.innen der Mitgliedsländer seit langem vertrauensvoll zusammenarbeiten.

Klingt nach Arbeit – aber Politik ist nun mal das „starke langsame Bohren von harten Brettern“.

Was auch immer gemacht wird – eins ist klar: An den entscheidenden Stellen brauchen wir Menschen mit Motivation zum Ermitteln, der Beharrlichkeit Fälle auszufechten und dem Willen Datenschutz und die Persönlichkeitsrechte der Bürgerinnen und Bürger durchzusetzen.

Nicht die Bürokratie ist das Problem, sondern die Menschen, die sich hinter ihr verstecken.

Liebe Helen Dixon,
dies ist keine Anfrage, keine Beschwerde, keine Klageeinreichung, kein Zwischenbescheid – das ist ein BigBrotherAward.

Die BigBrotherAwards sind unabhängig. Wir bekommen kein Geld vom Staat, wir nehmen kein Sponsoring von Google, Facebook & Co. – die BigBrotherAwards leben durch die privaten Spenden von tausenden von Menschen, die unsere Arbeit unterstützen. Wie wichtig unsere Unabhängigkeit ist, das zeigt uns genau dieser BigBrotherAward.

Herzlichen Glückwunsch, Helen Dixon und der ganzen irischen Datenschutzaufsicht zum Preis fürs Lebenswerk.

Congratulations, Ms. Dixon and the Irish Data Protection Commission – the BigBrotherAward 2022 for Lifetime achievement is yours.

1 The Journal, 3.5.2014: The Data Protection Commissioner is getting a new office, but keeping the one beside a convenience store in Laois https://www.thejournal.ie/data-protection-commissioner-new-office-1488473-May2014/

2 Zitat Wikipedia: Ireland's base erosion and profit shifting (BEPS) tools give some foreign corporates Effective tax rates of 0% to 2.5% on global profits re-routed to Ireland via their tax treaty network. (...) Ireland's BEPS tools are the world's largest BEPS flows, exceed the entire Caribbean system, Quelle: https://en.wikipedia.org/wiki/Ireland_as_a_tax_haven

3 Quelle Wikipedia: https://en.wikipedia.org/wiki/Corporation_tax_in_the_Republic_of_Ireland

4 Zitat aus der Parlamentsdebatte: It was interesting that when Matt Carthy put that to the Minister's predecessor, his response was that this was very unpatriotic and he should wear the green jersey. That was the former Minister's response to the fact there is a major loophole, whether intentional or unintentional, in our tax code that has allowed large companies to continue to use the double Irish. The Minister's predecessor has acknowledged the reputational damage this has done to Ireland. He was not really concerned about losing tax revenue and all the rest, but about the reputational damage. Let there be no doubt that, as we close one loophole and create another door, or do not close the door, this reputational damage is going to continue. Quelle: Dáil Éireann debate - Thursday, 23 Nov 2017, Vol. 962 No. 2. https://www.oireachtas.ie/en/debates/debate/dail/2017-11-23/18/

5 The Irish Times, 22.2.2022: Taoiseach defends Irish data protection commissioner in Germany – Martin doesn't 'readily agree' with many criticisms of Helen Dixon's record https://www.irishtimes.com/business/technology/taoiseach-defends-irish-data-protection-commissioner-in-germany-1.4809442

6 LIBE Ausschuss – Antrag auf Vertragsverletzungsverfahren vom 13.1.2021: Draft Motion for a resolution – B9-0000/2021 European Parliament Resolution on the ruling of the ECJ of 16 July 2020 - Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems ("Schrems II") - Case C-311/18 (2020/2789(RSP))

7 Im gerade fertiggestellten Digital Services Act (DSA) hat man die Lehren aus der DSGVO gezogen und die Aufsicht anders geregelt.

8 engl. European Data Protection Board, EDPB – das ist die Organisation, die früher „Artikel 29 Arbeitsgruppe“ hieß.

Pressemitteilung vom 15.02.2022

Netzwerk Datenschutzexpertise fordert Totalreform des Ausländerzentralregisters

Das Netzwerk Datenschutzexpertise hat ein umfangreiches Gutachten zum Gesetz über das Ausländerzentralregister (AZRG) erstellt, das zu einem vernichtenden Ergebnis kommt: Das AZRG verstößt in dutzendfacher Hinsicht gegen das deutsche Grundgesetz, gegen die europäische Grundrechte-Charta und gegen die europaweit geltende Datenschutz-Grundverordnung.

Im allgemeinen Datenbestand des Ausländerzentralregisters (AZR) werden teilweise hochsensitive Daten von allen in Deutschland lebenden ca. 11 Mio. ausländischen Menschen sowie von weiteren 8 Mio. Nichtdeutschen gespeichert. Die dort gespeicherten Daten werden nicht nur von Ausländer- und Asylbehörden angeliefert, sondern auch von Polizeien und Nachrichtendiensten, Sozial- und Gesundheitsbehörden. Alle Behörden in Deutschland und in der Europäischen Union haben einen Zugriff auf die dort gespeicherten Daten, die Polizeien und Nachrichtendienste haben einen praktisch unbeschränkten und nicht oder kaum kontrollierten direkten Zugriff auf sämtliche AZR-Daten. Transparenz für die Betroffenen besteht nur eingeschränkt und teilweise überhaupt nicht.

Statt diese Missstände zu beheben wird das AZR auf Grund eines Beschlusses der alten Großen Koalition ab November 2022 weiter ausgebaut: Ab dann sollen dort fast alle für die Betroffenen konfliktgeneigten ausländerrechtlichen und sämtliche asylrechtlichen Entscheidungen im Wortlaut verfügbar gemacht werden, um automatisiert von vielen Behörden, insbesondere auch von Sicherheitsbehörden, abgerufen werden zu können. Dies soll der erste Schritt dazu sein die bisherige dezentrale digitale Aktenführung der Ausländerbehörden zentral im AZR zusammenzuführen. Die Konsequenzen der Nutzung dieser Informationen können für die Betroffenen existenziell sein, indem sie z.B. für eine Abschiebeentscheidung herangezogen werden oder wenn aus einem Asylverfahren stammende Informationen an Verfolgerbehörden im Heimatstaat gelangen.

Trotz dieser gewaltigen Risiken sind die für die Betroffenen eingerichteten Schutzmaßnahmen entweder nicht existent oder unzureichend. Es erfolgt keine Unterrichtung über die Speicherung; der datenschutzrechtliche Auskunftsanspruch wird eingeschränkt; rechtliches Gehör ist nicht vorgesehen. Damit werden grundlegende Vorgaben des Datenschutzes wie der Rechtstaatlichkeit verletzt.

Das Gutachten des Netzwerks Datenschutzexpertise kommt zu dem Ergebnis, dass zunächst eine umfassende Evaluation des AZR erfolgen muss, um die – bisher nicht bekannte – tatsächliche Nutzung des Registers überschauen zu können. Auf dieser Grundlage muss dann das AZR einer Totalrevision unterzogen werden; die Regelungen des AZRG müssen auf das grundrechtlich tolerierbare Maß zusammengestrichen werden, so Thilo Weichert von Netzwerk Datenschutzexpertise:

„Bisher – seit über 25 Jahren – verweigert sich die Bundespolitik einer grundlegenden Überarbeitung des AZR, obwohl die verfassungsrechtlichen Mängel von Anfang an bekannt sind. Diese Mängel waren auch Thema eines weiteren aktuellen Gutachtens der Gesellschaft für Freiheitsrechte. Die Ampelkoalition und die neue Bundesregierung sind angetreten eine moderne Datenschutzpolitik und eine weltoffene und liberale Migrationspolitik zu praktizieren. Zentraler Bestandteil dieser neuen Politik muss die Reform des Ausländerzentralregisters sein. Glaubwürdigkeit beim Schutz von Menschenrechten beweist sich dort, wo die Betroffenen bisher keine Lobby und keine öffentliche Stimme haben. Bürgerrechtsorganisationen – auch das Netzwerk Datenschutzexpertise – helfen gerne dabei das AZR auf einen grundrechtskonformen Weg zu bringen.“

Das Gutachten ist im Internet abrufbar unter:
https://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2022_azrg.pdf.



Pressemitteilung von Digitalcourage vom 25.02.2022

1.000 Hilfsangebote für Schulen zu datenschutzfreundlichem Unterricht



Bild: Digitalcourage, Dennis Blomeyer, CC-BY 4.0, Erweitertes Bildformat

Im Sommer 2021 hat der gemeinnützige Verein Digitalcourage ein neues Hilfsprojekt für Schulen gestartet: Im „Netzwerk Freie Schulsoftware" finden alle Rat und Hilfe, die die schulische, digitale Bildung von Kindern bestmöglich und datenschutzfreundlich begleiten möchten.

- Ein politisch viel diskutiertes Thema

Eine besondere Herausforderung und Dauerthema in der Bildungspolitik ist die Bereitstellung geeigneter Unterrichtssoftware. Programme wie Microsoft Office, Teams, Zoom, Dropbox, One Drive oder Google Docs sind für die Nutzung an Schulen höchst umstritten, aus unterschiedlichen Gründen jedoch weiterhin vielerorts im Einsatz. Bund und Länder haben die Problematik zwar erkannt, die Bereitstellung von Alternativen, sowie Aufklärung über Datenschutz, laufen trotzdem nur schleppend an. Es gibt viele Schulen, die sich den Herausforderungen bereits gestellt und einen guten Umgang mit quelloffener, lizenzfreier und datensparsamer Software gefunden haben. Diese Schulen werden im Netzwerk Freie Schulsoftware mit anderen Schulen, Lehrkräften und Eltern zusammengebracht, die diesbezüglich aufholen möchten.

- Schulen helfen Schulen – so funktioniert es

Freiwillige Helferinnen und Helfer, meist Lehrkräfte oder Informatiker.innen, bieten über die Projektseite https://digitalcourage.de/netzwerk-freie-schulsoftware Erfahrungsaustausch oder Bedienungs- und Installationshilfe zu Freier Software an. Hinter den Kontaktdaten versteckt sich somit ein riesiger Fundus an Erfahrungen und Expertise. Schulträger, Schulleitungen, Lehrende und Eltern können sich gezielt an diese Personen wenden und sich bei den ersten Schritten helfen lassen. Auch allgemeines Informationsmaterial zu der Thematik steht auf der Projektseite bereit. Gibt es noch kein passendes Hilfsangebot für ein spezifisches Anliegen? Dann können Suchende das in einem Online-Formular vermerken, damit Digitalcourage e.V. seine Fühler nach passender Hilfe ausstrecken kann – ein geschlossener Kreislauf.

Die Vorteile:

- Durch die direkte Kontaktmöglichkeit gibt es keine weiteren organisatorischen Hürden.
- Viele der Helfer.innen kennen die Bedürfnisse, Probleme und Dienstwege an Schulen aus eigenen Erfahrungen.
- Die Kontaktpersonen möchten tatkräftig helfen – ganz unkompliziert, kostenfrei und aus Überzeugung.

- Ein voller Erfolg

Mittlerweile sind über 1.000 Hilfsangebote zu über 150 verschiedenen Programmen eingegangen: eine richtige Schatztruhe an geeigneter Unterrichtssoftware. Es gibt Hilfestellungen zum digitalen, gemeinsamen Arbeiten, Kommunizieren, Visualisieren und Lernen. Unter den eingetragenen Programmen befinden sich viele absolut notwendige, aber auch ein paar Dienste für spezielle Anwendungsfelder, wie Videoschnitt- oder Bildbearbeitungsprogramme.

- Mithilfe gesucht

Nun ist es wichtig, dass viele Schulen von den Angeboten erfahren und die Hilfe an genau den Stellen ankommt, die sie benötigen. Digitalcourage e.V. bittet um Hilfe bei der Verbreitung des Hilfsprojekts, z.B. durch Verteilen von Informationsmaterial, das über die Projektseite bezogen werden kann.

Pressekontakt: Jessica Wawrzyniak, Digitalcourage e.V., Tel: 0521 1639 1639 presse@digitalcourage.de

(Übersetzter) Offener Brief von EDRi und anderen vom 17.03.2022 zur geplanten Verordnung zur Bekämpfung des Kindesmissbrauchs

Sehr geehrte Kommissionspräsidentin Ursula von der Leyen,
sehr geehrte Vizepräsidentin Margrethe Vestager,
sehr geehrte Vizepräsidentin Vera Jourová,
sehr geehrte Vizepräsidentin Dubravka Šuica,
sehr geehrte Kommissarin Ylva Johansson,
sehr geehrter Kommissar Thierry Breton,
sehr geehrter Kommissar Margaritis Schinas,

Betreff: Schutz digitaler Rechte und Freiheiten bei der Gesetzgebung zur wirksamen Bekämpfung von Kindesmissbrauch

Die Bekämpfung der Online-Verbreitung von Material über sexuellen Missbrauch und sexuelle Ausbeutung von Kindern (CSAM) ist ein wichtiger Teil des umfassenderen globalen Kampfes zum Schutz junger Menschen vor sexuellem Missbrauch und sexueller Ausbeutung. Dieser Kampf erfordert einen umfassenden Ansatz von Regierungen und Unternehmen, um solche ungeheuerlichen Verbrechen zu verhindern, bevor sie passieren. Im Zusammenhang mit der bevorstehenden EU-Gesetzgebung zur wirksamen Bekämpfung von Kindesmissbrauch fordern wir die Kommission nachdrücklich auf dafür zu sorgen, dass die private Kommunikation der Menschen nicht zum Kollateralschaden der anstehenden Gesetzgebung wird.

Die schockierenden Ereignisse der letzten drei Wochen haben deutlich gemacht, dass Privatsphäre und Sicherheit sich gegenseitig verstärkende Rechte sind. Angegriffene Personen sind auf Technologien angewiesen, die die Privatsphäre wahren, um mit Journalisten zu kommunizieren, den Schutz ihrer Familien zu koordinieren und für ihre Sicherheit und ihre Rechte zu kämpfen. Auch in Friedenszeiten ist die Fähigkeit der Menschen ohne ungerechtfertigte Eingriffe zu kommunizieren – online wie offline – von entscheidender Bedeutung für ihre Rechte und Freiheiten sowie für die Entwicklung dynamischer und sicherer Gemeinschaften, der Zivilgesellschaft und der Industrie.

Wir sind der festen Überzeugung, dass wir zusammenarbeiten müssen, um langfristige Lösungen für die Verbreitung von CSAM online zu finden, die auf Beweisen beruhen und alle Grundrechte und die Rechtsstaatlichkeit respektieren. Wir glauben, dass der Rückgriff auf schnelle technologische „Lösungen" mit „Wundermitteln" nicht nur ineffektiv ist, sondern zu unbeabsichtigten Folgen für die Privatsphäre und Vertraulichkeit der Kommunikation jeder einzelnen Person führen, einschließlich der von Kindern und Missbrauchsbetroffenen. Die Experten sind sich einig, dass es keine Möglichkeit gibt Strafverfolgungsbehörden außergewöhnlichen Zugriff auf Ende-zu-Ende verschlüsselte Kommunikation zu gewähren ohne Schwachstellen zu schaffen, die Kriminelle und repressive Regierungen ausnutzen können. Die jüngsten Pegasus-Skandale haben gezeigt, dass das ungehinderte Abhören der Geräte von Menschen enorme Risiken birgt für Journalisten, Politiker, Menschenrechtsverteidiger und für den Erhalt der demokratischen Gesellschaft.

Die 35 unterzeichnenden Organisationen fordern daher die Europäische Kommission auf dafür zu sorgen, dass die bevorstehende Gesetzgebung zumindest eine Reihe von zehn sich ergänzenden Menschenrechtsprinzipien respektiert, von denen wir die folgenden hervorheben:

1. Keine Massenüberwachung: Es darf niemals ein allgemeines, automatisiertes Scannen der privaten Kommunikation Aller geben, da dies gemäß dem Wesen des EU-Rechts eine unverhältnismäßige Praxis ist. Die Gesetzgebung zur wirksamen Bekämpfung des sexuellen Missbrauchs von Kindern darf Dienstleister nicht zu Maßnahmen oder zur Sicherstellung von Ergebnissen veranlassen, die sie tatsächlich zum Durchführen solcher Mittel zwingen würden.
2. Eingriffe in die private Kommunikation von Personen müssen auf Grund eines individuellen Verdachts erfolgen: Jeder Eingriff in private Kommunikation muss, um gerechtfertigt zu sein, gemäß einer gesetzlichen Regelung und unter richterlicher Aufsicht auf der Grundlage eines konkreten, begründeten und individuellen Verdachts gerechtfertigt sein.
3. Die Maßnahmen müssen so wenig wie möglich in die Privatsphäre eingreifen und sich auf die Erkennung von CSAM beschränken: Um dies zu gewährleisten, sollte der Europäische Datenschutzausschuss (EDPB) Leitlinien zu geeigneten Technologien bereitstellen. Maßnahmen, die die Verschlüsselung brechen oder untergraben (z. B. Client-Side Scanning) oder die Cybersicherheitsrisiken schaffen, schaffen weit mehr Probleme, als sie lösen können.

Zivilgesellschaftliche Organisationen sind an der Gestaltung der Datenschutz-Grundverordnung (DSGVO), der kommenden ePrivacy-Verordnung und der Verhinderung illegaler Regelungen zur Vorratsdatenspeicherung beteiligt. Wir glauben daher, dass eine engere Zusammenarbeit bei dem bevorstehenden Vorschlag dazu beiträgt eine Gesetzgebung zu gewährleisten, die für ihren Zweck

wirksam, notwendig und verhältnismäßig ist. Dies trägt dazu bei, dass Rechtsstreitigkeiten vermieden werden, die Teile der geplanten Verordnung aufheben, die Diensteanbieter dazu zwingen würden ohne begründeten Verdacht in die private Kommunikation von Menschen einzudringen.

Als Verteidiger der Menschenrechte mit Technikkompetenz weisen wir erneut auf die inhärenten Grenzen jeder technologiebasierten „Lösung" von komplexen kriminellen Problemen wie die Verbreitung von CSAM hin, die einen ganzheitlichen Ansatz erfordern. Um das Ziel zu erreichen Kinder zu schützen, einschließlich der Verhinderung der Entstehung von CSAM, sind soziale und menschliche Interventionen mindestens so intensiv zu untersuchen wie technologiebasierte.

In einer Gesellschaft, die Demokratie und Rechtsstaatlichkeit respektiert, dürfen Regierungen nicht Maßnahmen um jeden Preis ergreifen. In einer Welt, in der jeder Aspekt unseres Lebens zunehmend digital wird, werden Maßnahmen zunehmend gefährlich, die die Privatsphäre und Vertraulichkeit der Kommunikation beeinträchtigen.

Wir hoffen, dass unsere Wortmeldung Ihnen bei den letzten Schritten der Gesetzgebung helfen. Wir stehen Ihnen hierbei mit Rat und Tat zur Verfügung.

Mit freundlichen Grüßen

Die unterzeichnenden Organisationen:

- European Digital Rights (EDRi)
- ApTI (Rumänien)
- Big Brother Watch (Großbritannien)
- Bits of Freedom (Niederlande)
- Center for Democracy and Technology (CDT) (International)
- Committee to Protect Journalists (CPJ) (International)
- Data Rights (Niederlande / Europa)
- dataskydd.net (Schweden)
- Defend Digital Me (Großbritannien)
- Deutscher Anwaltverein (DAV) (Deutschland)
- Deutsche Vereinigung für Datenschutz (DVD) (Deutschland)
- Digitalcourage (Deutschland)
- Digitale Gesellschaft (Deutschland)
- Državljan D/Citizen D (Slowenien)
- Electronic Frontier Foundation (EFF) (International)
- Electronic Frontier Finland (Effi) (Finnland)
- Entropia (Deutschland)
- European Center for Not-for-Profit Law (ECNL)
- European Sex Workers' Rights Alliance (ESWA)
- Foundation for Information Policy Research (FIPR) (Großbritannien / European)
- Global Voices (Niederlande / International)
- Homo Digitalis (Griechenland)
- Internet Society Catalan Chapter (ISOC-CAT) (Europa)
- ISOC Brazil - Brazil Chapter of the Internet Society (Brasilien)
- IT-Pol Denmark (Dänemark)
- LGBT Technology Partnership (International)
- Ligue des droits humains (Belgien)
- Mnemonic (Deutschland / International)
- Open Governance Network for Europe
- Open Rights Group (ORG) (Großbritannien)
- Privacy and Access Council of Canada
- Privacy International (PI)
- Ranking Digital Rights (International)
- Tech for Good Asia
- Vrijschrift.org (Niederlande)

Das englischsprachige Originaldokument kann im Netz abgerufen werden unter https://edri.org/our-work/private-communications-are-a-cornerstone-of-democratic-society-and-must-be-protected-in-online-csam-legislation/ (siehe auch den Hintergrund-Bericht auf S. 111).

Leserbrief

zu: „Mehr Fortschritt wagen – Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit", „Datenschutz Nachrichten" 1/2022, S. 18 ff.

Das Nötige tun, dem Möglichen widerstehen

Die noch recht neu im Amt befindliche „Ampel"-Koalition ist in nahezu allen Politikgebieten durchaus in der Lage lange verschleppte Reformen endlich auf den Weg zu bringen. Denn sie verbindet im Gegensatz zu vorherigen Bündnissen verschiedene Flügel und Ideologien miteinander, die somit ein Handeln nicht nur auf dem kleinsten gemeinsamen Nenner möglich machen, sondern tatsächlich weitreichende Transformationen anstoßen können. Dies gilt auch für den Bereich der Digitalisierung und des Datenschutzes: Mit dem Anteil der FDP als einer Verteidigerin der Freiheits- und Persönlichkeitsrechte einerseits, dem Anspruch der „Grünen" zum Schutz der Bürgerrechte und der vermittelnden Position der SPD mit dem Wunsch nach einem angemessenen Spielraum des Staates zur Aufrechterhaltung von innerer Sicherheit und Reglementierung andererseits, sind zwar die Vorzeichen für schwierige Verhandlungen schon jetzt durchaus gesetzt. Allen beteiligten Parteien ist allerdings der Wert sensibler Daten von deutlich größerem Ansinnen als der bisher an der „Großen Koalition" mitwirkenden CDU/CSU.

Zweifelsohne hat man im Koalitionsvertrag recht, wenn beispielsweise die DSGVO als ein wesentliches Rüstzeug und als Rahmen für künftige Einzelge-

setze angesehen wird. Gleichermaßen hat sich das Regelwerk auch Jahre nach seinem Inkrafttreten noch an vielen Stellen als wenig praxisnah herausgestellt. Die Diskussion darüber, wie größtmögliches Abschirmen von persönlichen Daten als grundgesetzlicher Auftrag mit dem Wunsch das Leben durch Erfassung, Speicherung und den Austausch solcher Persönlichkeitsmerkmale einfacher gestalten zu wollen, vereinbar ist, erfordert insofern Feingefühl und muss abgewogen stattfinden. Denn die Offenherzigkeit der Menschen mit ihren ureigenen Angaben immer öfter hausieren zu gehen und sie in sozialen Netzwerken einer breiten Öffentlichkeit unbedacht zur Verfügung zu stellen, ist tendenziell schon wieder rückläufig. Stattdessen haben die verschiedensten Skandale um die Zweckentfremdung von Daten durch Internetgiganten zu einem gesellschaftlichen Umdenken und einer neuen Selbstkritik in der Haltung der Bevölkerung gegenüber den eigenen Ansprüchen beigetragen.

Zweifelsohne: Datenschutz muss an den geeigneten Stellen Hürden aufstellen, um in einer modernen Welt aus Datenfluten die missbräuchliche Nutzung sensibler Informationen auf ein vertretbares Maß zu reduzieren. Gleichsam dürfen Datenschutzgesetze gerade in heiklen und non-profitablen Bereichen nicht zu einer derart ausgeuferten Bürokratie führen, dass wirksames Arbeiten mit notwendigen Daten verunmöglicht wird. Und so sind Forderungen von Vereinen und gemeinnützigen Organisationen nach Entlastungen im Datenschutz nachvollziehbar. Unmissverständlich zurückgewiesen werden müssen dagegen Überlegungen auf europäischer Ebene die Erfassung von biometrischen Komponenten weiter zu forcieren und deren Sammlung in Datenbanken sogar zu zentralisieren.

Ohnehin: In der Strafverfolgung und unter dem Vorwand der inneren Sicherheit darf es nicht zu weiteren Beschneidungen der persönlichen Integrität kommen. Im Zweifel muss das Verfassungsgericht dort auch künftig Grenzlinien ziehen, denn die Datensammelwut kann sogar auf die Meinung der Parteien übergreifen, die bislang als Bollwerk im Schutz vor dem gläsernen Bürger galten.

Letztendlich hoffe ich, dass sich die neue Koalition mit manch exekutiver Entscheidung, bei der es um die Daten von uns allen geht, deutlich schwerer tut als die „Durchwink“-Koalition aus Union und SPD der Vergangenheit, die viele Brüsseler Vorgaben unkommentiert passieren ließ. Dass Digitalisierung hilfreich sein kann, beweist die Lehre aus der aktuellen Corona-Pandemie deutlich: Wir hätten uns an vielen Stellen leichter getan und sicher manches Leben retten können, wenn Deutschland bereits stärker vernetzt gewesen wäre. Doch auch bei dieser Forderung darf es – wie bei jeder politischen Intervention – keine einfachen Antworten geben: Solange Datenverarbeitung im Verhältnis steht und überdies einer Mehrheit der Menschen zum unmittelbaren Nutzen ist, kann sie ein Segen sein. Gleichermaßen wird sie zum Fluch, wenn nicht mehr das Nötige zu ihrer Regulierung getan wird, sondern die Gier nach Machbarem selbstredend überwiegt.

Dennis Riehle, Konstanz



Bild: iStock.com/ golubovy

Datenschutznachrichten

Datenschutznachrichten aus Deutschland

Bund

Anonymous gegen Rosneft-Niederlassung

Bei einem Angriff auf die deutsche Niederlassung des russischen Energiekonzerns Rosneft hat das Hackerkollektiv Anonymous angeblich 20 Terabyte an Daten abgegriffen und die Inhalte auf Dutzenden Geräten gelöscht. Bei den erbeuteten Daten handele es sich um „Festplattenimages von Mitarbeiterlaptops und -Rechnern, Festplattenimages eines Mailservers, viele Archiv-Dateien, [...] Software-Pakete, Anleitungen, Lizenzschlüssel für Software“. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bestätigte über einen „IT-Sicherheitsvorfall“ informiert worden zu sein. Die Behauptungen von Anonymous kommentierte das BSI nicht. Rosneft ist Russlands größter Ölproduzent, Aufsichtsratschef ist trotz des Ukraine-Kriegs weiterhin Ex-Bundeskanzler Gerhard Schröder (SPD).

Gelungen ist der Zugriff gemäß den veröffentlichten Screenshots Anfang März 2022, also wenige Tage nach Beginn des russischen Angriffskriegs auf die Ukraine. Die Hacker konnten demnach nicht nur äußerst weit in die internen Systeme des Konzerns vordringen, sondern dann auch mit großer Geschwindigkeit Daten abziehen. Wegen der großen Menge von insgesamt fast 25 Terabyte habe das trotzdem lange gedauert. Am 04.03.2022 sei die Verbindung dann abgebrochen, warum wisse man nicht. Am 10.03.2022 sei dann erneut eine Verbindung hergestellt und der Download wieder aufgenommen worden. Bevor der dann wieder abgebrochen worden sei, habe man dank des direkt erratenen Security-PINs „1234“ noch 59 Apple-Geräte bei Rosneft zurückgesetzt und Datenbanken gelöscht. Die Daten sollen nun analysiert, aber nicht veröffentlicht werden.

Der deutsche Ableger des größten russischen Ölproduzenten war nach eigenen Angaben in den vergangenen Jahren für rund ein Viertel aller Rohölimporte nach Deutschland zuständig. Deswegen gehört das Unternehmen zur Kritischen Infrastruktur mit den zugehörigen Meldepflichten. Vorfälle wie der angebliche Einbruch in die IT müssen dem BSI mitgeteilt werden. Das erfolgte der Behörde zufolge einen Tag nach der Veröffentlichung der Details auf anonleaks.nl. Das BSI war seitdem in Kontakt mit Rosneft und gab eine „Cyber-Sicherheitswarnung an andere Unternehmen und Organisationen der Mineralölwirtschaft heraus“. Es seien keine Auswirkungen auf die Versorgungslage gefunden worden. Laut AnonLeaks hatten die Hacker „zu keinem Zeitpunkt Zugriff auf kritische Systemteile oder Steuerungsanlagen“, daran habe man auch kein Interesse gehabt (Holland, Angeblich 20 Terabyte abgezogen: Hackerangriff auf deutsche Tochter von Rosneft, www.heise.de 14.03.2022, Kurzlink: https://heise.de/-6548744).

Bund

EU-Vertragsverletzungsverfahren wegen Nicht-Umsetzung der DSRl-JI

Die EU-Kommission wirft der Bundesrepublik Deutschland vor die EU-Richtlinie zum Datenschutz in den Bereichen Polizei und Justiz (DSRl-JI) nicht komplett umgesetzt zu haben und hat ein weiteres Vertragsverletzungsverfahren in der Sache eingeleitet. Sie verweist diesmal auf fehlende Vorgaben für die Bundespolizei. Mit dem Erhalt des blauen Briefs hat die Bundesregierung zwei Monate Zeit, um auf das Schreiben zu reagieren und die notwendigen Maßnahmen zu ergreifen. Sie muss damit die von der Kommission festgestellten Verstöße gegen das EU-Recht abstellen. Andernfalls droht die Brüsseler Regierungsinstitution in der zweiten Stufe des Verfahrens eine „mit Gründen versehene Stellungnahme“ zu übermitteln.

Die Richtlinie wurde zeitgleich mit der stärker im öffentlichen Fokus stehenden Datenschutz-Grundverordnung (DSGVO) verabschiedet und in Kraft gesetzt. Sie schützt das Grundrecht der Bürger auf Privatheit, wenn Strafverfolgungs- und Gefahrenabwehrbehörden personenbezogene Daten verarbeiten. Die EU-Vorschriften sollen mit ähnlichen Betroffenenrechten wie in der DSGVO gewährleisten, dass personenbezogene Informationen von Opfern, Zeugen und Verdächtigen angemessen geschützt werden.

Der Bundesdatenschutzbeauftragte Ulrich Kelber hatte den Gesetzgeber Anfang 2021 ermahnt die Bestimmungen endlich in nationales Recht zu gießen. Deutschland habe schon damals die Umsetzungsfrist um 1.000 Tage überschritten. Er könne Datenschutzverstöße so etwa bei der Bundespolizei „nur beanstanden“, wirksame Durchsetzungsbefugnisse fehlten. Der Bundestag hatte im Juni 2021 zwar einen Entwurf zur Reform des Bundespolizeigesetzes beschlossen, mit dem auch die EU-Vorgaben umgesetzt worden wären. Der Bundesrat billigte die Initiative, die etwa eine Befugnis zum Einsatz von Staatstrojanern enthielt, aber nicht. Er rieb sich vor allem an den damit verknüpften weiten Einschnitten in die Kompetenzen der Länderpolizeien. Die Kommission hatte in dem Umsetzungsstreit bereits 2020 ein erstes Verletzungsverfahren gegen Deutschland vorangetrieben. Dabei ging es darum, dass fünf der 16 Bundesländer noch keine Maßnahmen ergriffen hatten (Krempl, Datenschutz bei Polizei: Neues EU-Vertragsverletzungsverfahren gegen Deutschland, www.heise.de 08.04.2022, Kurzlink: https://heise.de/-6666483).

Bundesweit

Schufa-Übernahme durch EQT im Streit

Das Bundeskartellamt (BKartA) mit Sitz in Bonn hat den Weg freigemacht für einen Verkauf der Schufa. Der Name des 1927 gegründeten Unternehmens steht für „Schutzgemeinschaft für allgemeine Kreditsicherung“. Das BKartA gab am 07.02.2022 grünes Licht für zwei Zusammenschlussvorhaben, die zwei Interessenten im Zusammenhang mit dem aktuellen Bieterwettbewerb um Anteile an der Wirtschaftsauskunftei angemeldet hatten. Der Präsident des BKartA, Andreas Mundt, erklärte dazu: „Wir prüfen in der Fusionskontrolle nur die wettbewerblichen Auswirkungen angemeldeter Zusammenschlüsse. Aus dieser Sicht waren beide Vorhaben freizugeben.“

Die eine der Initiativen hatte der schwedische Finanzinvestor EQT 2021 gestartet. Er will bis zu 100% der Anteile und damit die alleinige Kontrolle über die Schufa erwerben. Im ersten Schritt wollen die Schweden die Anteile der französischen Société Générale für 200 Mio. Euro erwerben und anschließend die weitere Übernahme vollziehen. Um dies zu verhindern, hat die TeamBank angekündigt ihre bestehende Minderheitsbeteiligung in Höhe von rund 18% an der Schufa aufzustocken. Sie gehört zur DZ-Bank-Gruppe. Bei ihr sind die Anteile der genossenschaftlichen Volks- und Raiffeisenbanken an der Auskunftei gebündelt. Die Schufa dient als Datenlieferant für die gesamte genossenschaftliche Finanzgruppe. Sie ist daher von hoher strategischer Bedeutung. Es liege, so die TeamBank, im Interesse der etablierten Anteilseigner stabile Mehrheitsverhältnisse zu erlangen, um die Neutralität der Auskunftei langfristig zu wahren.

Auch wenn beide Zusammenschlüsse und ihre Vorhaben in Konkurrenz zueinander stehen, ist es laut den Kartellwächtern unter bestimmten Umständen möglich solche Pläne parallel zur Fusionskontrolle anzumelden. Sie müssten dazu unter anderem hinreichend definiert sein. Durch die jetzigen Freigaben haben beide Bieter die Möglichkeit die Übernahmen fusionskontrollrechtlich zu vollziehen. Dem Fortgang des Bieterwettbewerbs liegen, so das BKartA, „allein unternehmerische Entscheidungen zugrunde“.

Mit einem Drei-Punkte-Papier für Verbraucherschutz wirbt die EQT für ihren Einstieg in den Kreditauskunftsdienst. In Gesprächen mit Verbraucherschützern, der Politik und Anteilseignern setzen die Skandinavier ein „Verbraucherschutz-Konzept für die Schufa“ ein. Die drei Kapitel des Dokuments umfassen Kulturwandel, Unternehmensführung sowie Verbraucherrechte und Datenschutz – wobei der letzte Teil die konkretesten Vorschläge enthält: unter anderem ein Portal, das dem Verbraucher unbeschränkten Gratiszugang zu seinen Daten gewähren soll. Nach Auskunft aus Finanzkreisen laufen unverändert Gespräche mit den Miteignern Deutsche Bank und Commerzbank.

- Datenschützer hat keine Probleme

Der hessische Datenschutzbeauftragte Alexander Roßnagel, der für die Schufa mit Sitz in Wiesbaden zuständig ist, äußerte keine Bedenken gegen einen Verkauf: „Datenschutzrecht gilt für die Schufa Holding AG unabhängig davon, wie die Aktionäre zusammengesetzt sind.“ Es könne für den Datenschutz von Vorteil ein, dass EQT die Transparenz der Datenverarbeitung für die betroffenen Personen etwa über ein „Datencockpit“ erhöhen wolle, eine stärkere Orientierung am Verbraucherschutz in Aussicht stelle und verspreche, dass Datensätze nicht außerhalb Europas gespeichert würden: „Hinweise, wie die Bonität verbessert werden kann, oder ein elektronisch gestütztes Beschwerdemanagement, in dem jede betroffene Person Fehler in den Daten einfach melden und korrigieren lassen kann, sind zukunftsweisend.“ Wer solche Pläne umsetze, „ist für den Datenschutz letztlich weniger entscheidend“.

Roßnagels Behörde hatte 2018 Pannen bei der Schufa aufgedeckt. Bei einigen Beschwerden ging es darum, dass „negative Bonitätsinformationen falschen Personen zugeordnet worden“ seien. Seit Jahrzehnten steht die Schufa in der Kritik, weil sie ihre für die Betroffenen existenziellen Scoreberechnungen nicht offenlegt, wegen aggressiver Werbung und beschönigender Selbstdarstellung, wegen einem hinhaltenden Service gegenüber den Betroffenen und wegen rechtswidriger Speicher- und Auskunftspraktiken. Der Europäische Gerichtshof (EuGH) prüft momentan, ob das Erstellen von Score-Werten der Schufa über Individuen und deren unkommentierter Transfer an Dritte wie Banken unter Art. 22 der Datenschutz-Grundverordnung (DSGVO) fällt (DANA 4/2021, 267). Dieser besagt, dass Personen prinzipiell „nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen“ werden dürfen.

- Eine dubiose Campact-Kampagne

Die Plattform Campact startete eine Kampagne, um den Verkauf der Schufa an EQT zu verhindern. Binnen weniger Tage unterzeichneten 219.781 Bürger den Appell an die Eigentümer der Auskunftei. Diese sollen demnach ihr Vorverkaufsrecht nutzen und dafür sorgen, dass keine Schufa-Anteile an undurchsichtige Investorengruppen gehen. EQT dürfe nicht Zugriff auf Profile von fast 70 Millionen Menschen in Deutschland bekommen. Der Konzern habe zwar erklärt Datenschutzinteressen konsequent zu verfolgen. Berichten zufolge gehe es ihm aber vor allem um Rendite, so Antonia Becher von Campact: „Schufa-Daten sind hochsensibel. Sie wirken sich auf unser Leben aus, entscheiden, ob jemand eine Wohnung bekommt, ein Haus bauen oder ein Unternehmen starten kann.“ Solche wichtigen Informationen dürften nicht zum Spielball von Finanzinvestoren werden. Zudem müsse die Schufa endlich transparent machen, „wie sie die Bonität von Menschen berechnet. Auch das ist bislang eine einzige Blackbox.“

Auf den Hinweis, dass die Angaben zur potenziellen Nutzung der Schufa-Daten durch EQT einfach falsch sind und dass die Planungen von EQT eine Verbesserung der Datenschutzsituation bei der Schufa versprechen, sah sich Campact nicht veranlasst seine Kampagne zu stoppen; wohl aber wurden die Angaben zum Datenschutz relativiert, so dass sie nicht mehr rechtlich angegriffen werden konnten.

Auf die Motivation zum Durchführen der Kampagne angesprochen, erklärte

Campact, diese gehe ausschließlich auf einen Zeitungsartikel zurück, in dem behauptet wird, es lägen „vertrauliche Unterlagen" vor, in denen EQT verspricht, die Schufa zu einem deutsch-europäischen Champion machen zu wollen, der die angelsächsische Dominanz im Bereich der Datenwirtschaft aushebeln soll. Letztlich schaue ein Finanzinvestor vor allem auf die Rendite. Was aus Datenschutzsicht gegen diese Planungen spricht, konnte und wollte Campact nicht offenlegen, ebenso wenig, wie das Kampagnenbüro die von EQT vorgeschlagenen Verbesserungen bei der Schufa bewertet.

Becher von Campact erklärte, die öffentliche Position von EQT werde durch die „internen Papiere, die kürzlich Medien zugespielt wurden" widerlegt: „Und die machen klar, dass es da hauptsächlich um höhere Rendite geht. EQT bleibt einfach ein Finanzinvestor, der mit diesen hochsensiblen Daten von 70 Millionen Deutschen neue datengetriebene Geschäftsmodelle machen und damit eben richtig dick Profit erwirtschaften will."

Auf Nachfrage teilte Campact mit die Unterlagen, welche EQT als Heuschrecke entlarven würden, selbst gar nicht zu kennen. Angesichts dessen muss das Vorgehen von Campact, das viele sinnvolle Kampagnen startet, hinterfragt werden, wenn es weniger um die Sache, als um Effekthascherei gehen sollte. Öffentliche kritische Kampagnen sollten gut recherchiert sein; im Fall von Fehlern sollte die Größe bestehen diese einzugestehen. Beides ließ Campact bei der EQT-Schufa-Kampagne vermissen.

- Politik mischt sich ein

Vor dem Hintergrund des Bieterstreits um die Schufa forderte Bundesverbraucherschutzministerin Steffi Lemke (Grüne) mehr Transparenz bei der Wirtschaftsauskunftei: „Wichtig für die Verbraucherinnen und Verbraucher ist vor allem, dass die Schufa transparenter wird. Dies hatte der Vorstand schon seit längerem angekündigt. Die Schufa ist eine privatwirtschaftliche Aktiengesellschaft mit mehreren unterschiedlichen Anteilseignern." Die Übernahme von Anteilen an der Schufa Holding AG werde unter den Anteilseignern und Bietern geklärt. Diese Entscheidung gelte es abzuwarten: „Egal, wie die Eigentümerstruktur am Ende aussieht, die europäischen und deutschen Datenschutz-Standards gelten für alle Unternehmen gleichermaßen. Es reicht nicht, dass man abfragen kann, welche Daten über einen gespeichert sind. Die Schufa sollte auch veröffentlichen, welche Informationen sie wie bewertet. Derzeit ist das Zustandekommen des Schufa-Scores immer noch eine Black Box."

Auch der digitalpolitische Sprecher der SPD-Bundestagsfraktion, Jens Zimmermann, kann dem möglichen Einstieg des Investors etwas Positives abgewinnen. Er glaube, es sei nicht ausgeschlossen, dass ein neuer Investor bei einem altehrwürdigen Unternehmen auch Innovation bringen könne: „Und ich glaube, man kann dieses Geschäftsmodell so betreiben, dass unsere Daten da sicher sind." Zimmermann gibt aber zu bedenken, dass EQT möglicherweise keine langfristigen Ziele verfolgt und seine Anteile später an den Meistbietenden verkaufen könnte. Wer auch immer das sei (vgl. schon DANA 4/2021, 240 ff.; Diesteldorf/Scheiber/Wischmeyer, Der Kampf um die Schufa, SZ 27.01.2022, S. 19; Smolka/Schönauer, EQT wirbt um Schufa mit Reformplan, www.faz.net, 28.01.2022; Krempl, Auskunftei Schufa: Kartellamt hat keine Bedenken gegen potenzielle Übernahme, www.heise.de 07.02.2022, Kurzlink: https://heise.de/-6352214; Ganswindt, Datenhandel: Schwedischer Investor will Schufa übernehmen, www.mdr.de 07.02.2022; Verbraucherministerin Lemke fordert Schufa zu mehr Transparenz auf, www.heise.de 09.02.2022, Kurzlink: https://heise.de/-6360100).

Bundesweit

Schufa kündigt Transparenzinitiative an

Die deutsche Auskunftei „Schufa" ist für die Verbraucher in Deutschland eine Black Box. Sie hat Daten über nahezu jeden Deutschen und entscheidet mit ihrer Bewertung der Kreditwürdigkeit darüber, ob Menschen einen Kredit für eine Immobilie bekommen oder einen Handyvertrag erhalten. Wie sich dieser Kreditscore zusammensetzt und wie die Menschen ihn verändern können, darüber rätseln in Deutschland auch Experten (siehe Meldung oben).

Tanja Birkholz, die neue Vorstandsvorsitzende des mächtigen deutschen Unternehmens, das in den letzten Jahrzehnten viel Kritik von Verbraucher- und Datenschützern einstecken musste, hat am 25.03.2022 eine Transparenzoffensive vorgestellt. Demgemäß soll in mehreren Schritten die Transparenz verbessert werden, indem die Auskunftei zunächst ihre Webseite und ihre Ansprache beispielsweise in Briefen an die Verbraucher ändert. Diese sollen einfacher, verständlicher und weniger fachjuristisch sein. Auf der Webseite soll es Erklärvideos zu den wichtigsten Fragen rund um die Schufa geben.

Als Herzstück der neuen Strategie wurde ein Simulator angekündigt, der erstmals in der langen Geschichte der Schufa nachvollziehbar machen solle, wie sich der Score der Auskunftei zusammensetzt, welche Merkmale wichtig sind und wie die Menschen die Bonitätsbewertung beeinflussen können. Die Schufa hatte sich bisher immer gegen solche Forderungen gewehrt mit der Behauptung, dass sich dadurch womöglich die Bewertung manipulieren ließe. Birkholz sieht das gemäß einer Präsentation jetzt angeblich anders. Der Score ist eine zentrale Geschäftsgrundlage der Schufa. Er bewertet die „Bonität" der Verbraucher: Wie hoch ist die Wahrscheinlichkeit, dass der oder diejenige einen neuen Kredit, das Haus oder die Wohnung auch zurückzahlen wird? Diese Information errechnet sich aus mehr als 100 Merkmalen, beispielsweise der Anzahl der Kreditkarten, Girokonten oder Kredite, die der Verbraucher in der Vergangenheit aufgenommen hat. Die Schufa gibt diesen Score an Unternehmen, die wissen wollen, ob ihr Kunde seine Rechnungen auch bezahlen kann. Deshalb ist er im Alltag der Menschen so wichtig.

Doch wie soll man ihn beeinflussen? Und warum ist er mal schlecht und mal gut? Dieses Rätsel will die Schufa nun ein wenig aufdecken und zeigte, wie ihr Simulator aussehen könnte. Bei diesem fragt die Schufa bei den Verbrauchern insgesamt sechs Merkmale ab, beispielsweise, wann er sein Bankkonto

eröffnet hat oder wie viele Kreditkarten er besitzt. Der Simulator errechnet anhand dieser Antworten, wie der aktuelle Score vermutlich gerade aussieht und ordnet ihn im Vergleich zur restlichen Bevölkerung ein. Aktuell arbeitet die Schufa dafür noch mit Schulnoten, will davon aber abrücken. Neben dem errechneten Beispielscore und der Einordnung soll der Simulator zeigen, wie sich der Score in den kommenden Monaten entwickeln wird, wenn der Verbraucher all seinen Verpflichtungen nachkommt. Auch Ereignisse wie einen Umzug sollen die Verbraucher im Schufa-Score simulieren können. All das soll dazu beitragen, dass die Black Box Schufa sich öffnet und Menschen besser verstehen, warum sie wie bewertet werden. Mittelfristig, so betont Birkholz, wollen sie zudem die Möglichkeit schaffen, dass die Verbraucher ihren eigenen Score in Echtzeit sehen und womöglich sogar beeinflussen können. Das sei aber nicht mehr für 2022 geplant, auch weil dafür noch viele Dinge zu klären sein, darunter einige Herausforderungen in der IT (Wischmeyer, Schufa will transparenter werden, SZ 26./27.03.2022, 28).

Bayern

VeRA-Zuschlag für Palantir

Palantir Technologies GmbH hat gemäß der Mitteilung des Bayerischen Landeskriminalamtes (BLKA) den Zuschlag für das „Verfahrensübergreifende Recherche- und Analysesystem" (VeRA) erhalten. Gemäß dem bayrischen Innenministerium habe kein anderes Unternehmen die „sehr strengen Ausschreibungskriterien" erfüllt. Die Analysten des BLKA sollen künftig das System der deutschen Tochter des umstrittenen US-Datenunternehmens Palantir zur Datenauswertung nutzen. Mit „VeRA" sollen bereits vorhandene Informationen aus verschiedenen, der Polizei zur Verfügung stehenden Datenbanken verknüpfbar gemacht werden. Dazu gehört, wie BLKA-Projektleiter Jürgen Brandl erklärte, das Vorgangsbearbeitungssystem, in dem alle Anzeigen und die dazugehörigen Sachverhalte gespeichert sind: „Unser Ziel ist, die Analysefähigkeit der Polizei zur Bekämpfung und Verfolgung der schweren und organisierten Kriminalität und des Terrorismus noch erfolgreicher und schneller zu machen." Neue Daten würden nicht erhoben.

Bayern soll damit gemäß den Angaben von BLKA-Präsident Harald Pickert Vorreiter für andere Bundesländer sein: „Die neue Software kann nicht nur in Bayern zum Einsatz kommen. Polizeien von Bund und Ländern haben jetzt die Möglichkeit, ohne zusätzliche aufwändige Vergabeverfahren dieses innovative Analysesystem zu nutzen." Bayern hat im Rahmen eines Bund-Länder-Vorhabens, das polizeiliche Verfahren vereinheitlichen soll, federführend die Ausschreibung übernommen und einen Rahmenvertrag geschlossen. Erneute Vergabeverfahren für die Polizeien von Bund und Länder sollen so vermieden werden.

Der bayerische Landesdatenschutzbeauftragte Thomas Petri sprach von einem massiven Eingriff in die Grundrechte von „Millionen Menschen". Die akten- und vorgangsübergreifenden „Big Data"- und Datamining-Verfahren erhöhten die Eingriffsintensität erheblich. Im Sommer 2020 hatte Privacy International vor Überwachungs-Outsourcing bei der Polizei gewarnt. Die Sicherheitsbehörden kooperierten häufig mit privaten Akteuren, darunter Palantir, um Bürger auszuspionieren. Dies verschlimmere Grundrechtseingriffe. Bereits bei der Ausschreibung zu „VeRA" waren Datenschutzbedenken laut geworden, sowie Bedenken angesichts einer möglichen Auftragsvergabe an Palantir, dem, so Petri, schwerlich vertraut werden könne. Der US-Mutterkonzern war für US-Geheimdienste und das Pentagon tätig und wird von Bürgerrechtlern und Datenschützern immer wieder kritisiert. Gegründet wurde Palantir von dem umstrittenen Tech-Milliardär Peter Thiel, der rechtsextreme Politiker, darunter den ehemaligen US-Präsidenten Donald Trump, finanziell unterstützt.

In Hessen und Nordrhein-Westfalen hat die Polizei in der Vergangenheit schon Erfahrungen mit Palantir-Software gesammelt. Im April 2020 plante Hessens Covid-19-Krisenstab mit einer Software des US-Unternehmens ein umfassendes Lagebild zur Corona-Pandemie zu erhalten. Später entschied sich die hessische Landesregierung jedoch dagegen. Anderthalb Jahre zuvor hatte Kritik an der Beschaffung und den Funktionen einer Palantir-Software der Polizei in Hessen für einen Untersuchungsausschuss gesorgt. Auch die Polizei von Nordrhein-Westfalen wollte Anfang 2020 das Datenanalyse- und Recherchesystem von Palantir einsetzen. Die Vergabe an Palantir ist Bestandteil des Aufbaus des bundesweiten „Datenhauses Polizei 2020", mit dem das bisherige Verbundsystem von Bund und Ländern INPOL (Informationssystem der Polizei) abgelöst werden soll. Das Bundeskriminalamt (BKA) erhielt für die Missachtung des Datenschutzes beim Aufbau von „Polizei 2020" im Jahr 2022 den BigBrotherAward in der Kategorie „Behörden und Verwaltung" (Knoblock, Bayerns LKA will umstrittene Palantir-Software einsetzen, www.heise.de 07.03.2022, Kurzlink: https://heise.de/-6541763; zum BigBrother-Award https://bigbrotherawards.de/2022/behoerden-verwaltung-bundeskriminalamt, siehe auch S. 92).

Bayern

Spyware Finfisher insolvent

Die Finfisher GmbH und zwei Partnerfirmen der Münchner Finfisher Holding GmbH – FinFisher Labs GmbH und raedarius m8 GmbH – haben nach einer Strafanzeige und anschließenden Kontopfändungen Insolvenz angemeldet und den Geschäftsbetrieb eingestellt. Im Rahmen des Ermittlungsverfahrens aufgrund illegaler Exporte des Staatstrojaners Finspy hat die Staatsanwaltschaft die Finfisher-Konten gepfändet. Vorangegangen war eine Strafanzeige der Gesellschaft für Freiheitsrechte e.V. (GFF), Reporter ohne Grenzen (RSF), des European Centers for Constutional and Human Rights (ECCHR) und Netzpolitik.org. Sarah Lincoln, Juristin und Verfahrenskoordinatorin der GFF erklärte: „Die Finfisher GmbH ist aufgelöst. Ihr Geschäft mit illegalen Exporten von Überwachungssoftware an repressive Regime ist gescheitert. Das ist ein direkter Erfolg unserer Strafanzeige."

Dem Global Spyware Index von 2021 zufolge war Finfisher Spyware-Marktführer und wird in 33 Ländern eingesetzt – dicht gefolgt von der ebenfalls stark kritisierten NSO Group. Lediglich

6% der Länder, in denen die Finfisher-Spyware eingesetzt wurde, sind gemäß dem Index echte Demokratien. Mit der Spyware von Finfisher und den Partnerfirmen des Unternehmens haben Polizei und Geheimdienste weltweit Menschen ausfindig machen, ihre Telefongespräche und Chats mitschneiden und sämtliche Handy- und Computerdaten auslesen können. Lisa Dittmer, Referentin für Internetfreiheit bei RSF: „Der Einsatz von Überwachungssoftware ist ein massiver Eingriff in die Persönlichkeitsrechte der Betroffenen, der insbesondere in Ländern mit repressiven Regimen dramatische Folgen haben kann – für Journalisten und ihre Quellen ebenso wie für Aktivistinnen und Oppositionelle."

Seit 2015 hat die Bundesregierung laut GFF keine Exportgenehmigungen mehr für Überwachungssoftware erteilt. Der Export derartiger Software für Länder außerhalb der EU ist genehmigungspflichtig und Verstöße sind strafbar. Dennoch tauchten immer wieder aktuelle Finspy-Trojaner in Ländern wie der Türkei auf. 2021 forderten ungefähr 100 Organisationen und Vereine in einem offenen Brief ein Moratorium für Spyware bis ein Rechtsrahmen verabschiedet und durchgesetzt wird, der die Durchführung einer menschenrechtlichen Sorgfaltsprüfung durchsetzt. Miriam Saage-Maaß, Legal Director beim ECCHR: „Bislang konnten Firmen wie Finfisher trotz europäischer Exportregulierung fast ungehindert weltweit exportieren. Die strafrechtlichen Ermittlungen waren längst überfällig und führen hoffentlich schnell zur Anklage und Verurteilung der verantwortlichen Geschäftsführer."

Die Münchner Staatsanwaltschaft ermittelt seit 2019 aufgrund mutmaßlichen Exports des Staatstrojaners. Damals hieß es, türkische Oppositionelle seien mit der Überwachungstechnik von Finfisher ausgespäht worden. Das Unternehmen warb mit dem „Kampf gegen Kriminalität". Es wurde vermutet, so die Staatsanwaltschaft, dass Finspy „ohne die erforderliche Ausfuhrgenehmigung des Bundesamtes für Wirtschaft und Ausfuhrkontrolle ausgeführt worden sein könnte". Inzwischen sei unter dem Firmennamen keiner mehr zu erreichen, die Briefkästen seien zugeklebt. An der Überwachungsmesse ISS World in Dubai Anfang März hatte Finfisher einer Messe-Sprecherin zufolge „nicht teilgenommen, nicht bezahlt und nicht abgesagt". Die Finfisher Holding GmbH wird zwar seit 2019 als Vilicius Holding GmbH weitergeführt, allerdings hat die Holding nichts mehr mit der Finfisher GmbH zu tun. Laut Insolvenzverwalter sind alle Mitarbeiter entlassen (Koch, FinFisher: Die Firma des Staatstrojaners „FinSpy" gibt es nicht mehr, www.heise.de 28.03.2022, Kurzlink: https://heise.de/-6655040).

Brandenburg

Polizeizugriff auf Luca-Corona-Aufenthaltsdaten

Die Polizei des Landes Brandenburg hat seit September 2020 Zugriffsrechte auf Gästelisten von Restaurants, Cafés, Hotels, Freizeiteinrichtungen und Geschäften sowie auf Mobilanwendungen, die aus der Corona-Kontaktnachverfolgung aus der Luca-App stammen. Möglicherweise in Unkenntnis dessen regte Brandenburgs Justizministerin Susanne Hoffmann (CDU) Anfang 2022 an im Kampf gegen schwere Verbrechen diese personenbezogenen Daten zu nutzen. Gemäß dem Polizeipräsidium Potsdam besteht eine mit der Generalstaatsanwaltschaft abgestimmte Regelung, „dass in einem solchen Falle der im konkreten Strafverfahren zuständige Verfahrensstaatsanwalt einen Entscheidungsvorbehalt hat".

Hoffmann hatte im Rechtsausschuss des brandenburgischen Landtags zwei Wochen zuvor noch von einer „unsicheren Rechtslage" gesprochen. Das Infektionsschutzgesetz des Bundes spreche nur vom „Ausschluss der Weiterverwendung von Verantwortlichen und zuständigen Stellen" und enthalte „keine Ausführungen zur Frage des Zugriffs von Strafverfolgungsbehörden". Es ist unklar, ob brandenburgische Ermittler Corona-Kontaktdaten tatsächlich abgefragt haben. Ein Sprecher des Polizeipräsidiums Potsdam erklärte, ihm persönlich sei kein Fall bekannt. Die Justizministerin meinte im Landesparlament, dass notfalls die Gerichte entscheiden müssten.

Das Bundesjustizministerium hält dagegen unter Verweis auf das Infektionsschutzgesetz den brandenburgischen Ansatz für klar rechtswidrig: Ein Zugriff auf Daten der Luca-App zu Zwecken der Strafverfolgung verstoße „gegen ausdrückliche Bestimmungen des Bundesrechts". Für Brandenburgs Datenschutzbeauftragte Dagmar Hartge ist die Rechtslage ebenfalls eindeutig: Die Kontaktdaten dürften nur erhoben und verarbeitet werden, „soweit dies zur Nachverfolgung von Kontaktpersonen zwingend notwendig ist". Die Verantwortlichen müssten sicherstellen, „dass eine Kenntnisnahme der erfassten Daten durch Unbefugte ausgeschlossen ist". Das Interesse der Strafverfolger sei zwar verständlich. Wenn der Rechtsstaat aber eine klare Ansage gemacht habe, „dann muss es auch so sein".

Die Firma Nexenio, die zusammen mit der Band Fanta4 hinter der Luca-App steht, reagierte auf die brandenburgische Debatte: „Daten sind nicht zentral in einem Luca-System lesbar gespeichert. Luca kann und will nicht auf die Daten der Kontaktnachverfolgung zurückgreifen und kann sie auch nicht an Ermittlungsbehörden rausgeben." Es sei nur im Infektionsfall möglich die Informationen zur Verfügung zu stellen. Und dies auch nur dann, „wenn das jeweilige Gesundheitsamt und der jeweilige Betrieb gleichzeitig ihr Einverständnis erteilen und ihre individuellen Schlüssel anwenden".

Eine Umfrage des Rundfunksenders rbb bei den Justizbehörden aller Bundesländer ergab, dass nur Bremen und Rheinland-Pfalz die Rechtsauffassung von Brandenburg teilen. Rheinland-Pfalz besteht demnach aber vor der Nutzung der Daten auf einem richterlichen Beschluss, seit der Mainzer Fall bundesweit für Aufsehen gesorgt hatte und der Landesdatenschutzbeauftragte das Vorgehen der Strafverfolger untersucht (DANA 1/2022, 38). Experten raten gegebenenfalls auf die Check-in-Funktion der Corona-Warn-App zu setzen. Dort ist aufgrund des dezentralen Ansatzes eine Datenabfrage nicht möglich (Krempl, Luca und Gästelisten: Polizei Brandenburg hat Lizenz für Datenabfragen, www.heise.de 24.02.2022, Kurzlink: https://heise.de/-6525210).

Bremen

Millionenbußgeld gegen Brebau wegen Diskriminierung

Die Bremer Datenschutzbeauftragte Imke Sommer hat auf Basis der Datenschutz-Grundverordnung (DSGVO) ein Bußgeld von 1,9 Millionen Euro gegen die Bremer Wohnungsbaugesellschaft Brebau verhängt, weil diese Mietinteressenten anhand überschüssiger Informationen in verschiedene Klassen einteilte und sich damit Rassismusvorwürfe einhandelte. Mehr als 9.500 Daten von Mietinteressenten habe die Brebau ohne Rechtsgrundlage verarbeitet. Dabei habe es sich etwa um Informationen über Frisuren, Körpergeruch und das persönliche Auftreten gehandelt, was für den Abschluss von Mietverhältnissen nicht erforderlich sei: „Bei mehr als der Hälfte der Fälle handelte es sich darüber hinaus um Daten, die nach der DSGVO besonders geschützt sind." Die Tochtergesellschaft der Stadt Bremen erfasste demnach auch Informationen über die Hautfarbe, die ethnische Herkunft, die Religionszugehörigkeit, die sexuelle Orientierung und über den Gesundheitszustand. Zudem habe die Brebau Anträge Betroffener auf Transparenz über die Verarbeitung ihrer Daten bewusst unterlaufen.

Reporter des regionalen TV-Magazins „buten un binnen" hatten 2021 aufgedeckt, dass das Unternehmen Menschen nach Herkunft und äußeren Merkmalen kategorisierte. Die Abkürzung E40 stand demnach etwa für Farbige. Ein Vermerk mit der Abkürzung KT legte nahe, dass Bewerberinnen Kopftuch trugen. Angesichts der „außerordentlichen Tiefe der Verletzung des Grundrechts auf Datenschutz" wäre laut Sommer eigentlich „eine deutlich höhere" Strafe angemessen gewesen. Davon habe sie abgesehen, weil die Brebau im Aufsichtsverfahren „umfassend kooperierte" und sich um Schadensminderung sowie eigene Aufklärung des Sachverhalts bemüht habe. Die öffentliche Gesellschaft habe zudem Maßnahmen ergriffen, „dass entsprechende Verstöße sich nicht wiederholen".

Auf Grund des Vorgangs mussten unter anderem zwei Führungskräfte gehen. Ein vom Aufsichtsrat beauftragter Sonderermittler kam zu dem Ergebnis, dass bei der Brebau kein struktureller Rassismus vorgeherrscht habe. Sommer erklärte, sie sei im Kontext der öffentlichen Diskussion über den Fall häufig gefragt worden, ob die DSGVO Diskriminierungen verbietet. Darauf gäbe es keine einfache Antwort, weil die Verordnung in spezifischer Weise auf Sachverhalte schaue. Prinzipiell sei es demnach aber nur in wenigen Ausnahmefällen überhaupt erlaubt Daten über Hautfarbe, ethnische Herkunft, Religionszugehörigkeit, sexuelle Orientierung und über den Gesundheitszustand zu verarbeiten. Gar nicht erst erhobene Informationen könnten folglich auch nicht missbraucht werden. In diesem Sinne schütze die DSGVO vor Diskriminierungen. Der Datenschutzexperte der FDP-Fraktion in Bremen, Magnus Buhlert, begrüßte die Sanktion: Es sei gut, dass die Aufsichtsbehörde „ohne Ansehen der juristischen Personen entschieden hat". Die Brebau müsse „auch als staatliches Unternehmen für ihre Verfehlungen geradestehen. Theoretisch wäre sogar eine höhere Strafzahlung möglich gewesen" (Krempl, Mieterdiskriminierung: Brebau muss knapp 2 Millionen DSGVO-Strafe zahlen, www.heise.de 04.03.2022, Kurzlink: https://heise.de/-6539624).

Nordrhein-Westfalen

Anwaltsdaten ungeschützt in Internet-Cloud

Der Anwalt Matthias Bauer, LL.M., bekannt dafür, dass er Darknet-Shopper, AfD-Politiker und Burschenschafter vertritt, hat Dokumente seiner Mandanten offen im Netz gespeichert. Brauer hat sich für seine Bonner Kanzlei unter anderem die Webseite darknet-anwalt.de gesichert: „Fernab von klassischem Strafrecht beschäftigte ich mich schon früh mit neuen Medien und betreute verstärkt Mandanten aus dem Bereich der Internetkriminalität." Dass seine Mandanten mit ihm offenbar bisher zufrieden waren, zeigt die Bewertung bei anwalt.de: 5 von 5 Sternen. Der Tageszeitung taz wurde aber bekannt, dass Brauer Unmengen vertraulicher Mandantenakten unverschlüsselt und ohne Passwortschutz über Dropbox, einem Cloud-Speicher, im Netz abgelegt hat. Über den Link konnten im Browser ohne weitere Hürden mehr als 1.500 Ordner der Kanzlei abgerufen werden, wobei in der Regel jedem Ordner ein Fall mit teils tausenden Seiten zugeordnet war. Die mehr als 100 Gigabyte an Daten umfassten den Zeitraum 2016 bis März 2022.

Es ist unklar, ob der Dropbox-Link öffentlich kursierte und wer evtl. Zugriff auf die Dateien nahm. Es handelt sich in jedem Fall um einen eklatanten Verstoß gegen den Datenschutz und das Anwaltsgeheimnis. Das Datenleck ist auch wegen der politischen Ausrichtung des Anwalts relevant. In den Daten finden sich Unterlagen zu Presserechts-Streitigkeiten, unter anderem mit der taz. Brauer vertritt etwa den rechtsextremen Verein „Ein Prozent", die rechtsextreme Identitäre Bewegung, rechte Burschenschaften und nach eigenen Angaben in mehr als 100 Fällen Fraktionen, Parteigliederungen und einzelne Politiker der AfD, auch in parteiintern Auseinandersetzungen, sowie einzelne rechte und rechtsextreme Personen wegen unterschiedlichen Straftaten. Auch die Daten mutmaßlicher Opfer standen offen im Netz, etwa private Daten von Personen, die gegen die AfD demonstriert haben.

Brauer arbeitet u.a. für die Kanzlei von Enrico Komning, der für die AfD im Bundestag sitzt und dem völkisch-nationalen Flügel der Partei zugerechnet wird. Brauer war auch selbst in der AfD aktiv, als Justiziar war er Mitglied des Landesvorstands Rheinland-Pfalz. Zuvor war er als Burschenschafter aufgefallen, der weit rechts außen steht. Nachdem er 2007 in Ku-Klux-Klan-Manier unter „Hail White Power"-Rufen ein Holzkreuz verbrannte, wurde Brauer aus der Burschenschaft Marchia Bonn ausgeschlossen. Er trat dann den radikaleren Raczeks in Bonn bei und ist auch Mitglied der Rugia Greifswald, bei der der Verfassungsschutz „rechtsextremistische Bezüge" sieht. Im 2011 begonnenen Richtungsstreit des Dachverbandes Deutsche Burschenschaft sprach sich Brauer für den „Arierparagraf" aus, nach welchem die Mitgliedschaft in einer Burschenschaft an völkische und rassistische Kriterien geknüpft werden sollte.

Rechtsanwälte sind als Berufsgeheimnisträger besonders verpflichtet vor-

sichtig mit ihnen anvertrauten Daten umzugehen. § 203 des Strafgesetzbuches sieht für die „Verletzung von Privatgeheimnissen" bis zu ein Jahr Haft oder Geldstrafe vor. Gemäß der Bundesrechtsanwaltsordnung ist Verschwiegenheit eine berufliche Grundpflicht, wozu es auch gehört die Daten zu den Mandanten sorgfältig zu schützen. In der Dropbox waren sensible Daten gespeichert: Adressen, Geburtsdaten und Telefonnummern von Mandanten, Notizen und Schriftsätze des Anwalts und Schreiben von Justizbehörden, komplette Ermittlungsunterlagen, die dem Anwalt im Zuge der Akteneinsicht zur Verfügung gestellt wurden, also etwa Befragungen von Beschuldigten, Opfern und Zeugen. Es geht um unterschiedliche, kleine und komplexe Fälle: Drogendelikte, Diebstahl, Betrug, Fahrerflucht, Körperverletzung und Sexualstraftaten einschließlich Fälle sogenannter Kinderpornographie.

Da die Dateien in einer Dropbox gespeichert sind bzw. waren, liegen sie in der Regel auf Servern in den USA, was mit europäischem Datenschutz prinzipiell nicht kompatibel ist, weil nicht ausgeschlossen werden kann, dass US-Behörden Zugang zu den Daten haben. Es gibt verschiedene einfache Möglichkeiten eine Dropbox so abzusichern, dass Unbefugte nicht durch simples Aufrufen eines Links darauf zugreifen können. Anwälte werden von Berufsverbänden und Kammern regelmäßig auf ihre Verantwortung für die Datensicherheit ihrer Mandantendaten hingewiesen. Die Dropbox wurde dafür benutzt von außerhalb des IT-Systems der Kanzlei auf Dokumente zugreifen zu können. Der Anwalt hatte den Link zu seiner Dropbox offenbar selbst verschickt, unter anderem an sein Sekretariat, wie sich aus Mails in der Dropbox ergibt. Auch Mandanten wurde demgemäß per Link Zugang zu einzelnen Unterordnern gewährt.

Die nordrhein-westfälische Datenschutzbeauftragte wurde über das Leak informiert. Der Sprecher der NWR-Datenschutzbehörde, Daniel Strunk, erklärte, nach Ermittlung und Bewertung des Sachverhalts werde man „die angemessenen Aufsichtsbefugnisse ausüben". Die Datenschutzbehörde kann hohe Bußgelder verhängen. Zudem müssen laut Datenschutz-Grundverordnung die betroffenen Personen vom Verantwortlichen informiert werden, sofern das Datenleck für sie voraussichtlich ein hohes Risiko zur Folge hat. Gemäß Strunk ist der Fall einzigartig; es habe in den vergangenen Monaten wohl eine Handvoll Meldungen von Steuerberatern, Kanzleien und Rechtsanwälten gegeben, bei denen um es um Hackerangriffe auf Mailserver ging – aber ohne Hinweise auf Datenabflüsse.

Karina Nöker, die Geschäftsführerin der für Brauer zuständigen Kölner Rechtsanwaltskammer, konnte sich auf Anfrage an keinen vergleichbaren Datenschutzverstoß von Anwälten erinnern: „Wir werden dies zum Anlass nehmen, ein berufsrechtliches Verfahren einzuleiten." Der Berliner Rechtsanwalt Niko Härting, beim Deutschen Anwaltsverein in den Ausschüssen für Informationsrecht, Berufsrecht sowie Berufsethik, meinte: „Das ist der Super-Gau, wenn Kanzlei-Daten in andere Hände geraten. Das darf nicht passieren" (Erb/Schulz, Nazi-Anwalt ohne Datenschutz, taz.de 31.03.2022, https://taz.de/taz-Recherche-zu-Leak-sensibler-Daten/!5845365/).

Saarland

Grethel erneut zur Datenschutzbeauftragten gewählt

Die Juristin Monika Grethel ist vom Landtag in Saarbrücken für weitere sechs Jahre zur Landesbeauftragten für Datenschutz und Informationsfreiheit im Saarland gewählt worden. Sie erhielt nach erfolgter Ausschreibung am 16.02.2022 von 44 abgegebenen 42 Stimmen. Grethel hat das Amt seit dem 01.04.2016 inne. Bevor die parteilose Juristin 2010 zur saarländischen Datenschutzaufsicht als Referatsleiterin stieß, war sie Verwaltungsrichterin. Sie leitet damit das Unabhängige Datenschutzzentrum Saarland als Aufsichtsbehörde des Bundeslands. Die Landesbeauftragte für Datenschutz überwacht die Einhaltung der Datenschutz-Vorschriften bei öffentlichen und nicht-öffentlichen Stellen. Jeder, der sich durch die Datenverarbeitung in seinen Rechten verletzt sieht oder der sein Recht auf Informationszugang durch eine öffentliche Stelle als verletzt ansieht, kann sich an die Landesbeauftragte wenden. Ihr stehen umfassende Auskunfts-, Einsichts- und Zutrittsrechte zu (Kirch, Monika Grethel erneut zur Datenschutz-Beauftragten des Saarlandes gewählt, www.saarbruecker-zeitung.de 16.02.2022; Schulzki-Haddouti, Datenschutzbeauftragte Saarland: Auf kleiner Flamme, www.iitr.de 30.11.2016).

Sachsen

Hundert folgt Schurig

Am 21.12.2021 wurde Frau Dr. Juliane Hundert als Nachfolgerin von Andreas Schurig zur Sächsischen Datenschutzbeauftragten gewählt. Schurig hatte das Amt seit 2004 inne. Die Sächsische Datenschutzbeauftragte ist für Sachsen die Datenschutz-Aufsichtsbehörde nach Artikel 51 Absatz 1 der Datenschutz-Grundverordnung (DSGVO). Dies ergibt sich im Hinblick auf nicht-öffentliche Stellen aus § 14 Absatz 2 des Sächsischen Datenschutzdurchführungsgesetzes (SächsDSDG); im Hinblick auf öffentliche Stellen aus § 14 Absatz 1 desselben Gesetzes.

Hundert legte im Juni 1995 ihr Abitur am Franziskaneum in Meißen ab. Von 1995 bis 2001 studierte sie Rechtswissenschaft an der Friedrich-Schiller-Universität Jena. Ihr anschließendes Referendariat in Dresden schloss sie 2003 mit dem 2. Juristischen Staatsexamen ab. Von 2003 bis 2004 war sie als angestellte Rechtsanwältin in Dresden, danach bis 2010 als Referentin beim Sächsischen Datenschutzbeauftragten tätig. 2009 promovierte Hundert zum Thema „Die Rückabwicklung des finanzierten Beitritts zu einer Publikumsgesellschaft" an der Friedrich-Schiller-Universität. Nach einer kurzen anschließenden Tätigkeit im Sächsischen Staatsministerium für Soziales war Hundert seit Januar 2011 als Parlamentarische Beraterin bei der Fraktion Bündnis 90/Die Grünen des Sächsischen Landtags in den Fachbereichen Innenpolitik, Kommunales, Datenschutz und Justiziariat tätig; seit 2015 leitete sie das Fraktions-Justiziariat (v.a. Wikipedia https://de.wikipedia.org/wiki/Juliane_Hundert).

Datenschutznachrichten aus dem Ausland

EU

Europol erhält mehr Kompetenzen

Das Kerngeschäft der europäischen Strafverfolgungsbehörde Europol mit ihren ca. tausend Mitarbeiterinnen und Mitarbeitern in Den Haag befasst sich vorwiegend damit Daten zu beschaffen, zu sichten und zu sortieren. Mit dem Erstellen von Lageanalysen helfen sie den Mitgliedstaaten der EU bei der Bekämpfung schwerer Formen der internationalen Kriminalität. Europol wurde 1998 gegründet und ist seit 2010 offiziell eine Agentur der Europäischen Union (EU). Je mehr sich die Kriminalität ins Internet verlagert, desto umfangreicher wird ihre Arbeit. Von Kritikern wird Europol als „Datenkrake" und „Datenmonster" bezeichnet, auch weil sich die Behörde mit ihrer Arbeit oft am Rand der Legalität bewegt. Dies soll nun geändert werden.

Vertreter des Europaparlaments und der 27 EU-Staaten haben sich am 01.02.2022 darauf geeinigt ihr Mandat u.a. im Umgang mit personenbezogenen Daten deutlich zu erweitern. Den ursprünglichen Vorschlag dafür hatte die EU-Kommission im Jahr 2020 unter dem Eindruck mehrerer terroristischer Anschläge gemacht. Die Behörde soll demnach Innovationstreiber auf dem Gebiet der Datenanalyse werden und Anwendungen der künstlichen Intelligenz für die Ermittlungsarbeit entwickeln. Sie soll mehr Kompetenzen bei der Analyse großer Datensätze bekommen. Wenn es um Terrorismus und Kindesmissbrauch geht, soll Europol auch Daten von Drittstaaten annehmen dürfen, egal welche Datenschutzbestimmungen dort gelten, ebenso Daten von Privatunternehmen. Das könnten z.B. soziale Netzwerke sein, die Chatprotokolle von verdächtigen Nutzern zur Verfügung stellen. Auch personenbezogene Angaben dürften von Europol angenommen werden.

Datenschützer sehen die neuen Regelungen als rückwirkende Legitimierung von illegalen Praktiken Europols. Der Europäische Datenschutzbeauftragte Wojciech Wiewiórowski hatte Europol erst einige Wochen vor der Einigung aufgefordert massenhaft vorhandene persönliche Daten – offenbar vier Petabyte aus laufenden und abgeschlossenen Ermittlungsverfahren – zu löschen, die der Behörde von den Mitgliedstaaten zugeschickt worden waren. Eigentlich müssten Daten von Personen nach sechs Monaten gelöscht werden, wenn keine Verbindung zu einer kriminellen Aktivität nachgewiesen werden kann. Es sieht aus, als habe die Behörde selbst den Überblick über den Wust an Informationen verloren. Das Büro von Wiewiórowski hatte im Jahr 2019 eine Untersuchung dazu eingeleitet, wie Europol mit persönlichen Daten verfährt, und die Behörde seither mehrmals zu Änderungen aufgefordert. Die Daten sind bis heute nicht gelöscht und dürfen offenbar im Rahmen der neuen Regeln weiterverwendet werden. Die neue Löschfrist soll 18 Monate betragen.

Die EU-Kommission und die Mitgliedsländer behaupten, sie würden mit der Änderung für Rechtssicherheit sorgen, so z.B. EU-Innenkommissarin Ylva Johansson: „Europol braucht moderne Mittel, um die Polizei bei ihren Ermittlungen zu unterstützen". Das vereinbarte Mandat bekräftige die Rolle der Agentur als globale Vorreiterin bei der Entwicklung neuer Technologien für die Strafverfolgung, bei Verhütung und Aufklärung von Straftaten, aber auch beim Schutz von Grundrechten wie dem Schutz personenbezogener Daten.

Der Europäische Datenschutzbeauftragte soll nur rückwirkend Einblick erhalten in die Art und Weise, wie die Behörde mit personenbezogenen Daten umgeht, was Amtsinhaber Wiewiórowski kritisiert: „Die Ausweitung der Befugnisse von Europol geht nicht Hand in Hand mit einer verstärkten Kontrolle der Maßnahmen der Agentur." Die im Vorschlag enthaltenen Bestimmungen seien eine „direkte Bedrohung" für die Rolle der Aufsichtsbehörde (Kelnberger, Freifahrtschein für Europol, SZ 03.02.2022, 6).

EU

Datenschutzbeauftragter kritisiert polizeiliche Datenaustauschpläne

Der EU-Datenschutzbeauftragte (EDSB) Wojciech Wiewiórowski fordert Korrekturen am Entwurf zur Erweiterung des Prümer Vertrags in Bezug auf den Austausch biometrischer Daten. Die Initiative der EU-Kommission für eine Verordnung „über den automatisierten Datenaustausch für die polizeiliche Zusammenarbeit", mit welcher der Prümer Vertrag von 2005 erweitert werden soll, schießt demnach über ihr Ziel hinaus. Ihr fehlten „wesentliche Elemente in Bezug auf seinen sachlichen und persönlichen Anwendungsbereich". Mit dem Prüm-Rahmen können Polizeibehörden in den angeschlossenen Mitgliedsstaaten DNA-, Fingerabdruck- und Fahrzeugregisterdaten elektronisch austauschen und abgleichen. Nationale Datenbanken werden vernetzt. Künftig sollen auch Fahndungsfotos oder biometrische Lichtbilder aus Polizeiregistern einbezogen werden, die eine automatisierte Gesichtserkennung unterstützen.

Die Kommission hat es gemäß Wiewiórowski versäumt die Arten von Straftaten, die eine Abfrage rechtfertigen können, zu bestimmen. Dies gelte auch für die Kategorien der Personen, die von dem automatischen Datenaustausch betroffen sind. Er verlangt, dass insbesondere der automatisierte Abruf von DNA-Profilen und Gesichtsbildern nur im Zusammenhang mit einzelnen Ermittlungen bei schweren Straftaten möglich sein sollte. Die Kommission will solche Abgleiche sensibler Daten bei sämtlichen Delikten zulassen. Darüber hinaus ist der EDSB nicht von der Notwendigkeit des in der „Prüm-II-Verordnung" vorgeschlagenen automatisierten Abrufs und Austauschs von Daten aus polizeilichen Aufzeichnungen überzeugt. Er unterstreicht, dass strenge Sicherheitsvorkehrungen erforderlich seien, um die damit verbundenen Risiken für die Datenqualität anzugehen.

Wiewiórowski äußerte schwere Bedenken bzgl. der Verhältnismäßigkeit des Vorhabens. Diese erstrecken sich auch auf die Einbeziehung von Europol in den Prüm-Ansatz. Die Polizeibehörde in Den Haag solle nur eingeschränkt Big-Data-Analysen durchführen dürfen. Ihm zufolge müssen die dortigen Ermittler künftig binnen sechs Monaten klären, ob es ihnen gestattet ist erhaltene personenbezogene Informationen längerfristig zu speichern und zu verwenden. Daten mit unklarem Status sind im Anschluss zu löschen. Die EU-Länder und das Europäische Parlament haben sich aber schon auf einen anderen Verordnungsentwurf verständigt, mit dem das Mandat für Europol deutlich ausgeweitet werden soll. Nach der Position beider Gremien werden die von der Aufsichtsbehörde als rechtswidrig gebrandmarkten Praktiken weitgehend legalisiert.

Teil des kritisierten Gesetzespakets der Kommission für die stärkere polizeiliche Kooperation ist auch ein Entwurf für eine Richtlinie über den Informationsaustausch. Wiewiórowski hält es hier für unerlässlich den persönlichen Anwendungsbereich der speziellen Befugnisse klar zu definieren. Auf jeden Fall müssten die Kategorien personenbezogener Daten über Zeugen und Opfer, die ausgetauscht werden können, begrenzt werden. Der Kontrolleur kritisiert zudem die geplante Dauer der Speicherung personenbezogener Daten in den Fallverwaltungssystemen der einheitlichen Ansprechpartner sowie die skizzierte Rolle von Europol beim Austausch personenbezogener Daten zwischen nationalen Strafverfolgungsbehörden. Die Mitgliedstaaten sollten laut der separaten Stellungnahme zu diesem Entwurf verpflichtet werden von Fall zu Fall zu beurteilen, ob Europol eine Kopie der von den zuständigen nationalen Behörden ausgetauschten Informationen erhalte. Dabei sei der Zweck klar anzugeben. Andernfalls könnte die Richtlinie dazu führen, dass „eine riesige Datenbank mit Sicherungskopien der ausgetauschten Informationen entsteht“. Eine solche würde von Europol für neue, von der Behörde selbst festgelegte Zwecke verwendet. Die polizeiliche Zusammenarbeit sei „ein wichtiges Element eines gut funktionierenden Raums der Freiheit, der Sicherheit und des Rechts“. Eine stärkere Rolle von Europol als „Informationsdrehscheibe“ müsse aber angemessen sein. Sie dürfe nicht „als Nebeneffekt zur Schaffung neuer großer zentralisierter Datenbanken führen“ (Krempl, Datenschutz: Plan für EU-weiten Abgleich von Gesichtsbildern sorgt für Unmut, www.heise.de 16.03.2022, Kurzlink: https://heise.de/-6550673).

EU

Umstrittene Bekämpfung des Kindesmissbrauchs im Netz

Seit Jahren wird darüber diskutiert, ob digitale Kommunikation nach missbräuchlichen Darstellungen von Kindern durchsucht werden muss oder darf, um dadurch den dokumentierten Kindesmissbrauch zu bekämpfen. Die EU-Kommission wird ihren hierzu geplanten Gesetzesentwurf voraussichtlich erst im Sommer präsentieren. Unbestritten ist, dass der Schutz der Kinder vor Missbrauch schon längst eine digitale Dimension hat. Die rasante Verbreitung der Darstellungen von sexualisierter Gewalt gegen Kinder ist ein großes Problem, das Kindesmissbrauch wiedergibt und zugleich anheizt. Es geht um die Frage, wieviel individuelle Freiheitsrechte man bereit ist für mehr Sicherheit vulnerabler Gruppen aufzugeben.

Die für März 2022 vorgesehene Präsentation eines Gesetzesentwurfs der Europäischen Kommission für ein Kinderrechtspaket verzögert sich. Kontrovers diskutiert werden insbesondere Pläne auch verschlüsselte digitale Kommunikation massenhaft und auf Verdacht nach Missbrauchsdarstellungen zu durchsuchen. Bereits 2020 sorgte die „freiwillige Durchsuchung“ von privaten Nutzernachrichten nach möglichen illegalen Inhalten durch Plattformkonzerne wie Google, Facebook und Microsoft für Debatten, als sie betroffenes Material aus nicht-verschlüsselter digitaler Kommunikation über Dritte wie das National Center for Missing & Exploited Children (NCMEC) in den USA oder direkt an die Strafverfolgungsbehörden weiterleiteten.

Nach Inkrafttreten des neuen Telekommunikationskodexes und der dadurch bedingten Anwendung der alten europäischen E-Privacy-Richtlinie stellten die Plattformen aus Sorge vor rechtlichen Problemen diese Praxis ein. Der EU-Gesetzgeber reagierte mit einer interimistischen Regulierung, die im Juli 2021 vom EU-Parlament bewilligt wurde. Diese temporäre Verordnung, die den Anbietern das Monitoring gestattet, läuft 2023 aus.

Wie eine endgültige Regelung gemäß einem Gesetzesentwurf EU-Kommission aussehen wird, ist noch unklar. Der EU-Parlamentarier Patrick Breyer (Piratenpartei) veröffentlichte im März 2022 eine Stellungnahme von EU-Innenkommissarin Ylva Johansson, wonach eine Verpflichtung der Messenger- und E-Mail-Dienste zum Durchsuchen nach missbräuchlichen Inhalten geplant ist. Bereits im November 2021 hatten die EU-Innenminister in einem gemeinsamen Statement eine solche Vorschrift in Aussicht gestellt. Ein neues EU-Zentrum zur Bekämpfung von Kindesmissbrauch soll hierbei als zentrale Meldestelle für die Anbieter fungieren und gewährleisten, dass das Monitoring durch die Tech-Konzerne nicht zu anderen Zwecken eingesetzt wird.

- Die Sicht der Datenschützer

Breyer befürchtet, dass dies letztlich eine „Massenüberwachung durch vollautomatisierte Echtzeit-Chatkontrolle und damit die Abschaffung des digitalen Briefgeheimnisses“ zur Folge hat: „Der angekündigte Gesetzesentwurf bedroht außerdem die sichere Verschlüsselung, denn auch Ende-zu-Ende-verschlüsselte Dienste sollen in Zukunft durchleuchtet werden.“ Er befürchtet die „Privatisierung“ der Strafverfolgung, da intransparente Algorithmen von Konzernen Verdachtsfälle bewerten müssten. Zudem sei der Einsatz von Künstlicher Intelligenz beim Durchforsten der digitalen Kommunikation nach inkriminierten Inhalten äußerst fehleranfällig: „Nach Angaben der Schweizer Bundespolizei sind 86 Prozent der maschinell angezeigten Inhalte nicht strafrechtlich relevant, wie etwa Urlaubsfotos am Strand mit nackten Kindern.“ Die technische Umsetzung eines Monitorings bei Ende-zu-Ende ver-

schlüsselter Kommunikation würde die Anbieter tatsächlich vor große Herausforderungen stellen.

Tom Jennissen vom Verein Digitale Gesellschaft meinte hierzu: „Technisch gesehen können derartige Maßnahmen bei Ende-zu-Ende-verschlüsselter Kommunikation mittels Messengern wie etwa Telegram oder Signal nur funktionieren, wenn die Verschlüsselung aufgehoben oder umgangen wird." Um diese technische Hürde zu meistern, fürchten er und andere Datenschützer die umfassende Anwendung eines sogenannten „Client-Side Scanning" (CSS), wonach die Inhalte nicht während des Versendens, sondern direkt auf den Endgeräten der Nutzenden geprüft würden, bevor die Verschlüsselung greift. Die vorgesehenen Maßnahmen würden nur funktionieren, wenn die Kommunikation der Nutzenden vollständig und in Echtzeit durchleuchtet würden. Schnell könnten solche Möglichkeiten „angesichts zunehmend autoritärer Tendenzen in einigen Mitgliedsstaaten" demokratiegefährdend zweckentfremdet werden, beispielsweise zur Überwachung politischer oder gesellschaftlicher Opposition: „Nicht erst die angespannte Weltlage sollte eigentlich allen politisch Verantwortlichen vor Augen führen, dass das Kompromittieren oder Unterlaufen von Ende-zu-Ende-Verschlüsselung eine ganz schlechte Idee ist. Denn selbstverständlich kann jede Sicherheitslücke nicht nur von Kriminellen, sondern auch von ausländischen Geheimdiensten genutzt werden."

Vor diesem Hintergrund veröffentlichten 39 Bürgerrechts- und Datenschutzorganisationen, darunter auch die Deutsche Vereinigung für Datenschutz, einen offenen Brief an die EU-Kommission, in dem diese eindringlich vor der Aufhebung der Ende-zu-Ende-Verschlüsselung warnen. Darin fordern sie ein klares Nein zur massenhaften Überwachung, eine Intervention in private Kommunikation nur im Verdachtsfall und eine ausschließliche Beschränkung auf missbräuchliche Darstellung von Kindern (siehe in diesem Heft S. 101).

- Die Sicht der Kinderschützer

Jutta Croll, Vorstandsmitglied der National Coalition Deutschland, ein Netzwerk zur Umsetzung der UN-Kinderrechtskonvention, sieht die Nachrichtendurchsuchung aus einem anderen Blickwinkel: „Das dringendste Anliegen aus kinderrechtlicher Perspektive ist es die Potenziale des digitalen Umfelds für Kinder – vor allem bei der Ausübung ihrer Rechte – nutzbar zu machen. Das ist dann zwangsläufig verknüpft mit der Gewährleistung des Schutzes von Kindern. Wenn dem nicht so ist, kann die Ausübung der Teilhaberechte, des Rechts auf Bildung, Zugang zu Informationen und freie Meinungsäußerung und vielem mehr nicht ausgeschöpft werden."

Zwar würden sich Datenschützer stark auf das Privatsphärerecht von Kindern beziehen, dieses sei jedoch allgemein „eines der ambivalentesten Menschenrechte überhaupt": „Bei Kindern kommen da zusätzliche Ebenen hinzu, weil sich die Eltern als Erziehungsverantwortliche auf Messers Schneide bewegen und ihren Kindern Privatsphäreschutz gewähren sollen." Das Client-Side Scanning biete den Vorteil, dass die Behörden damit nicht nachlaufend reagieren müssten, was der effizientere Weg sei. Sie räumt ein: „Ich bin mir durchaus bewusst, dass man das als Privatsphäreverletzung bezeichnen kann." Aktuell sei durch das Client-Side Scanning jedoch nicht die gesamte private Kommunikation betroffen; tangiert seien ausschließlich mit Hashes gekennzeichnete Inhalte, die bereits als inkriminiertes Material bekannt seien. Solche Hashes von bekanntem inkriminiertem Material werden in einer Datenbank von Europol erzeugt, nachdem eine Meldung eingegangen ist und validiert wurde, dass es sich tatsächlich um illegales Material handelt.

Mit Ende-zu-Ende-Verschlüsselung könne, so Croll, dieses Vorgehen jedoch nicht mehr weiterhelfen: „Hier setzen Kinderrechtsadvokat:innen an, zu sagen, dann kann Verschlüsselung kein sinnvolles Instrument sein, wenn sie genau an dieser Stelle den Schutz verhindert". Deshalb sei das proaktive Monitoring auf dem Endgerät der Nutzenden erforderlich. Wenn klar sei, dass Ende-zu-Ende-Verschlüsselung das Mittel der Wahl ist, dann brauche es die Bereitschaft und die technischen Möglichkeiten bei den Plattformbetreibern trotzdem weiter Monitoring zu betreiben.

Croll kritisiert auch das bisherige Vorgehen der europäischen Regulierungsverantwortlichen: „Ich war entsetzt, dass man aus dem Trilog und den Verhandlungen zur DSGVO nicht die Lehren gezogen hat und mit der E-Privacy-Regulierung in dieselbe Falle getappt ist. Nämlich kurz vor Schluss zu merken, dass eine in guter Intention auf den Weg gebrachte Initiative möglicherweise Seiteneffekte hat und Kollateralschäden verursachen kann." Das Inkrafttreten des EU-Telekommunikationskodex und das dadurch abgeschaltete Monitoring der großen Plattformen habe zu einem starken Rückgang der Meldungen von missbräuchlichen Darstellungen geführt: „Das National Centre for Missing and Exploited Children spricht von einem Rückgang der Meldungen aus Europa um 50 bis 60% im Vergleich zum Vorjahr." Wenn man bedenke, dass die Gesamtzahl der Missbrauchsdarstellungen während der Pandemie laut BKA um 53% gestiegen ist, wäre eigentlich ein entsprechender Anstieg auch der Meldungen zu erwarten gewesen. Dies habe auch dazu geführt, dass man eine Interimsregulierung auf den Weg gebracht habe. Es müsse jedenfalls bis zum Ende dieser temporären Regelung ein neuer Ansatz gefunden werden, um eine Wiederholung dessen zu verhindern (Müller, Wie lassen sich Kinderrechte und Privatsphäre schützen? Tagesspiegel Background Digitalisierung&KI, 23.03.2022).

EU

Von der Leyen und Biden kündigen neues Privacy-Shield an

EU-Kommissionspräsidentin Ursula von der Leyen und US-Präsident Joe Biden haben in Brüssel eine „grundsätzliche Einigung" über den transatlantischen Datenverkehr erzielt, so dass zwischen der Europäischen Union (EU) und den USA personenbezogene Daten wieder einfacher fließen können. Nach einem Gipfelgespräch mit US-Präsident Biden hat von der Leyden einen neuen Ansatz zum Datenaustausch angekündigt. Sie freue sich sehr, „dass wir eine

grundsätzliche Einigung über einen neuen Rahmen für den transatlantischen Datenverkehr erzielt haben." Ein neues Abkommen werde „vorhersehbare und vertrauenswürdige" Datenflüsse ermöglichen, bei denen die Privatsphäre und die Bürgerrechte geschützt werden. Biden zeigte sich „stolz" über den „weiteren großen Durchbruch" beim Datenverkehr: „Die EU-Kommission kann nun wieder transatlantische Datenflüsse erlauben", die Geschäfte im Wert von 7,1 Mrd. Dollar ermöglichten – der Gesamtwert der jährlichen Geschäfte zwischen beiden Seiten.

Ein Entwurf für eine neue rechtliche Rahmenvereinbarung existiert bisher offenbar noch nicht. Die Anforderungen an ein solches „Datenschutzschild" sind hoch: Der Europäische Gerichtshof (EuGH) hatte im Sommer 2020 mit dem „Schrems II"-Urteil den transatlantischen Privacy Shield und damit eine der wichtigsten Grundlagen für den Transfer von Kundendaten in die USA für ungültig erklärt (DANA 3/2020, 199ff.). Die Luxemburger Richter hatten dabei erneut festgestellt, dass US-Gesetze wie der Foreign Intelligence Surveillance Act (FISA) oder der Cloud Act eine Massenüberwachung durch Sicherheitsbehörden ermöglichen und der Datenschutzstandard in den Vereinigten Staaten nicht dem in der EU entspricht. 2015 hatte der österreichische Aktivist Max Schrems vor dem EuGH auch bereits das Vorgängerabkommen „Safe Harbor" zu Fall gebracht. Ein dritter Anlauf dürfte daher ohne grundsätzliche US-Reformen wohl kaum ausreichen, um einen angemessenen Datenschutz für EU-Bürger zu gewährleisten.

Gemäß einem „Faktenblatt" der Kommission soll ein „neues Regelwerk" „verbindliche Garantien" enthalten, um den Zugriff von US-Geheimdiensten wie der NSA auf persönliche Daten von EU-Bürgern „auf das zu beschränken, was zum Schutz der nationalen Sicherheit notwendig und verhältnismäßig ist". US-Sicherheitsbehörden würden der Absprache zufolge „Verfahren einführen, die eine wirksame Kontrolle der neuen Datenschutz- und Bürgerrechtsstandards gewährleisten". Dazu komme ein „neues zweistufiges Rechtsbehelfssystem zur Untersuchung und Beilegung von Beschwerden von Europäern über den Zugriff auf Daten durch US-Geheimdienste". Dieses werde ein spezielles Gericht zur Prüfung solcher Eingaben umfassen.

Die Kommission spricht zudem von „strengen Auflagen für Unternehmen, die aus der EU übermittelte Daten verarbeiten". Diese schlössen weiterhin die Pflicht zu einer Selbstzertifizierung ein, wonach sie die einschlägigen Grundsätze des US-Handelsministeriums befolgten. Weiter habe man „spezifische Überwachungs- und Überprüfungsmechanismen" vereinbart. Insgesamt würden die „in die USA übermittelten Daten der Europäer unter Berücksichtigung" des Schrems-II-Urteils des EuGHs (DANA 3/2020, 199 ff.) geschützt.

Schrems sieht die Ankündigung von der Leyens skeptisch: „Wir hatten bereits 2015 ein rein politisches Abkommen, das keinerlei Rechtsgrundlage hatte. Wie es derzeit aussieht, könnten wir das gleiche Spiel jetzt ein drittes Mal spielen." Bei dem Deal handle es sich offenbar um einen symbolischen Schritt, der „keinen Rückhalt der Experten in Brüssel hat, da sich die USA nicht bewegt haben". Nach Informationen der von Schrems gegründeten Datenschutzorganisation Noyb planen die USA „keine Änderungen ihrer Überwachungsgesetze, sondern lediglich Zusicherungen der Exekutive" über einschlägige Anordnungen. Diese hätten „keine externe Wirkung und können nicht eingeklagt werden". Eine echte Lösung wie ein „No-Spy-Abkommen" mit „Basisgarantien unter gleichgesinnten Demokratien" sei hier bisher nicht ersichtlich. Kunden und Unternehmen drohten so „weitere Jahre der Rechtsunsicherheit".

Zuvor hatte eine Entscheidung des Obersten Gerichtshofs der USA, des Supreme Court, der US-Regierung mehr Spielraum bei der Berufung auf „Staatsgeheimnisse" in Spionagefällen eingeräumt. US-Bürgern und Europäern dürfte es so gleichermaßen schwerer fallen eine geheime Überwachung durch Sicherheitsbehörden in den USA vor dortigen Gerichten anzufechten.

Eine neue Vereinbarung wäre wieder eine Exekutiventscheidung der EU-Kommission, die zunächst vom Europäischen Datenschutzausschuss (EDSA) geprüft werden müsste. Dieser Prozess kann erst nach Vorliegen eines Entwurfs für einen solchen Rechtsakt gestartet werden. Bis zum Angemessenheitsbeschluss der Kommission dürfte es noch ein paar Monate brauchen. Bis dahin können sich Unternehmen nicht auf die reine Ankündigung berufen. Dennoch lobte der europäische Arbeitgeberverband Business Europe die „Einigung" als „tolles Signal an die Business-Community und die ganze Welt". Die internationale Datenschutzvereinigung IAPP (International Association of Privacy Professionals) kommentierte, nun könnten „Datenschutz-Profis auf der ganzen Welt endlich aufatmen".

Rebekka Weiß vom Digitalverband Bitkom erklärte, die politische Einigung sei „nur der dringend notwendige erste Schritt: Jetzt gilt es diesen politischen Willen in eine belastbare rechtliche Regelung zu überführen." Die Firmen bräuchten „rasch Rechtssicherheit, damit die bestehende Datenblockade endlich aufgelöst werden kann". Gerade auch kleinere Unternehmen seien „auf die Speicherung von Daten in der Cloud, Nutzung der Software US-amerikanischer Anbieter und Kommunikation in sozialen Netzwerken und die Nutzung von Videokonferenzsystemen internationaler Anbieter angewiesen".

Der Vize-Fraktionsvorsitzende der Grünen im Bundestag, Konstantin von Notz, begrüßte die Grundsatzerklärung, nachdem die Kommission und die vorherige Bundesregierung dem Grundrechteschutz der Menschen in Europa sowie der notwendigen Rechtssicherheit für die Wirtschaft jahrelang nicht gerecht geworden seien. Die Brüsseler Regierungsinstitution müsse nun ihrer Verantwortung gerecht werden und dafür Sorge tragen, dass das neue Abkommen einen echten Mehrwert etwa für die informationelle Selbstbestimmung der Nutzer biete und auf „immer neue Hilfskonstrukte" verzichte (Krempl, Privacy Shield 2.0: EU und USA einig bei neuem Abkommen zum Datenaustausch, www.heise.de 25.03.2022, Kurzlink: https://heise.de/-6634101; Brühl, Daten-Drama, dritter Akt, SZ 26./27.03.2022, 28; Krempl, Privacy Shield 2.0: USA geloben „beispiellose" Überwachungsreform, www.heise.de 26.03.2022).

EU

EDSA macht Vorgaben gegen „Dark Pattern"

Der Europäische Datenschutzausschuss (EDSA) hat im März 2022 Empfehlungen zum Schutz von Social-Media-Anwendern vor dem Missbrauch ihrer persönlichen Daten verabschiedet. Mit „Dark Pattern" werden Benutzerschnittstellen und Nutzungsvorgaben bezeichnet, die darauf ausgelegt sind die Nutzenden zu Handlungen zu verleiten, die ihren Interessen entgegenlaufen. Die nun vorliegenden offiziellen Vorgaben zur Vermeidung von Dark Patterns gelten bei der Gestaltung von und beim Umgang mit Social Media in der gesamten Europäischen Union (EU). Sie umfassen praktische Empfehlungen für Designer und Nutzer der Plattformen. Das Ziel besteht darin Verstöße gegen die Datenschutz-Grundverordnung (DSGVO) zu verhindern.

Dark Patterns auf den Social-Media-Plattformen können Nutzende dazu verleiten persönliche Daten unabsichtlich und mit möglicherweise schädlichen Folgen preiszugeben. Die Richtlinien geben konkrete Beispiele für Dark Patterns und bewährte Vorgehensweisen für die datenschutzfreundliche Gestaltung von Social-Media-Inhalten in unterschiedlichen Anwendungsfällen. Der Bundesdatenschutzbeauftragte Ulrich Kelber begrüßte diese „positive Entwicklung": „Ausspionieren darf kein Geschäftsmodell in Europa sein. Wenn soziale Medien die Daten ihrer Nutzenden verwenden wollen, dann dürfen diese nicht mit unfairen Mitteln zur Einwilligung gedrängt werden" (Ungerer, Datenschutz: europäische Richtlinien gegen „Dark Patterns", www.heise.de 16.03.2022, Kurzlink: https://heise.de/-6549591).

Belgien/EU

Bußgeld für die IAB Europe wegen Real Time Bidding

Die belgische Datenschutzbehörde Autorité de protection des données (APD) hat einen für die Onlinewerbung zentralen Standard, das „Transparency & Consent Framework" (TCF) für datenschutzrechtlich unzulässig erklärt und der Werbe-Organisation IAB Europe ein Bußgeld von 250.000 Euro auferlegt. Zudem wurde die IAB aufgefordert alle gesammelten Daten zu löschen. Die Entscheidung erging nach dem „One Stop Shop"-Prinzip der Datenschutz-Grundverordnung (DSGVO) und gilt somit für die gesamte EU.

Das TCF ist der zentrale Standard hinter Cookie-Bannern und personalisierter Werbung. Kernaufgabe des TCF ist die Weitergabe des Einverständnisses in die Datenverarbeitung zu Werbezwecken. Sobald Nutzende bei einem Cookie-Banner auf „Akzeptieren" klicken, wird ein sogenannter TC-String erzeugt und an alle Partner geschickt, die am sogenannten OpenRTB-System (Real Time Bidding) teilnehmen. Aufgrund dieses TC-Strings werden Nutzerprofile zusammengestellt, die dann die Grundlage für Echtzeit-Werbeauktionen bilden, mit denen einzelne Werbeplätze unter oft Hunderten Firmen versteigert werden.

In ihrer mit den europäischen Datenschutzbehörden abgestimmten Entscheidung halten die belgischen Datenschützer fest, dass nicht nur die Werbeprofile, sondern bereits der TC-String als personenbezogenes Datum gelten muss, da der String mit der IP-Adresse kombiniert werden kann, um die Nutzer identifizierbar zu machen. Diese Feststellung ist ein Debakel für die Werbeindustrie, weil diese TC-Strings nach den Regeln der DSGVO behandelt werden müssen. Das bedeutet nicht nur, dass Nutzer informiert zustimmen müssen, damit diese Daten problemlos übertragen werden können. Benötigt wird auch ein offizieller Verantwortlicher, der für die Datenweiterverarbeitung Tausender Firmen geradesteht.

Die IAB Europe hatte bereits in den vergangenen Monaten klargemacht, dass sie diese Rolle nicht einnehmen will. Das TCF wurde gerade deshalb als „freiwilliger Standard" konstruiert, um eine solche Haftung zu vermeiden. Doch wer an dem System nicht teilnimmt, muss im Werbegeschäft mit erheblichen Verlusten rechnen. Die Datenschützer haben auch mit der konkreten Ausgestaltung des TCF Probleme. Die Kategorien, denen die Nutzer bei Cookie-Bannern zustimmen sollen, sind laut der Entscheidung viel zu vage, als dass den Nutzenden klar werden könnte, welchen Umfang die Datenweitergabe im Hintergrund hat. Es besteht für sie keine Möglichkeit die Datenverarbeitung effektiv nachzuvollziehen.

Der für das Verfahren zuständige Datenschützer Hielke Hijmans erklärte: „Menschen werden aufgefordert ihre Zustimmung zu geben, aber die meisten von ihnen wissen nicht, dass ihre Profile viele Male am Tag verkauft werden, um ihnen personalisierte Werbung zuzuteilen." Die IAB Europe erhielt mit der Entscheidung zwei Monate Zeit zu erklären, wie sie das System auf eine legale Basis stellen will.

- IAB Europe wehrt sich

Die IAB Europe hat angekündigt gegen diese Entscheidung vor Gericht Klage einzureichen. Insbesondere wendet sich die Organisation gegen die Feststellung, dass sie als „Controller" für die Daten verantwortlich sein soll. Darüber hinaus betont IAB Europe, dass nicht das TCF an sich, sondern die konkrete Ausgestaltung für unzulässig befunden wurde. Man sei optimistisch innerhalb eines halben Jahres mit der Behörde eine für beide Seiten zufriedenstellende Lösung zu finden.

Die Branchenorganisation IAB Europe fungiert als zentrale Schaltstelle, um die Zustimmungen zu Datenverarbeitungen aus Cookie-Bannern an Werbemarktplätze zu übermitteln. Die belgischen Datenschützer haben zwar nicht die technische Umsetzung insgesamt für illegal erklärt, sehen aber die IAB Europe als Co-Controller der Daten, die zur Erstellung von Nutzerprofilen genutzt werden können.

Dieser juristische Befund hat große Auswirkungen. IAB Europe meinte als kleiner Branchenverband unmöglich die Verantwortung für die Datenverarbeitung aller Empfänger dieser Daten übernehmen zu können. Auf der offiziellen Liste der Datenempfänger stehen derzeit 794 Firmen, die wiederum die Daten an eine unbekannte Anzahl weiterer Firmen weitergeben können. Die Beschwerdeführer unterstellen, dass es bereits genügt, an den täglich milliardenfach stattfindenden Werbeauktio-

nen teilzunehmen, um personalisierte Daten abzuschöpfen.

Da Endnutzer für illegale Datenverarbeitung zu Werbezwecken Schadensersatz verlangen könnten, wäre das Kostenrisiko für IAB Europe unkalkulierbar. Dabei geht es um Milliardenumsätze. Laut verschiedenen Branchenstatistiken werden mittlerweile über zwei Drittel der Online-Werbung mit Hilfe personalisierter Werbeprofile ausgespielt, bereits 2019 betrugen die Ausgaben in diesem Markt laut IAB Europe 23 Milliarden Euro – mit stark steigender Tendenz. Diesen Umstand versuchen sich die Beschwerdeführer nun zunutze zu machen.

- Auslöser: Bürgerrechtsorganisationen

Das Verfahren geht auf eine Beschwerde des Irish Council for Civil Liberties (ICCL) und anderer europäischer Bürgerrechtsorganisationen zurück (siehe dazu das Schwerpunktheft DANA 3/2019). ICCL-Vertreter Johnny Ryan meinte: „Die heutige Entscheidung befreit Hunderte Millionen Europäer von dem Konsens-Spam und von der tieferen Gefahr, dass ihre persönlichsten Daten unter Tausenden von Firmen herumgereicht werden." Das Milliardengeschäft mit personalisierter Werbung könne nach der Entscheidung der belgischen Datenschützer nicht wie bisher funktionieren. Derweil arbeitet die Werbebranche daran das Geschäftsmodell zu retten. Bereits im Vorfeld der Entscheidung hatte die IAB Europe begonnen sich auf die neuen Gegebenheiten einzustellen. So wurde ein Programm zur „Vendor Compliance" aufgelegt, das die Bedenken gegen die Weitergabe von Werbeprofilen an hunderte Bieter ausräumen soll. Kritiker wie Ryan halten diesen Versuch allerdings für aussichtslos, da die Daten viel zu weit gestreut würden, um eine wirkungsvolle Kontrolle ausüben zu können.

Obwohl die belgischen Datenschützer der IAB zwei Monate Zeit gegeben haben, um ihre Verbesserungspläne einzureichen, versuchen das ICCL und das Electronic Privacy Information Center (EPIC) den Beschluss bereits jetzt durchzusetzen. Sie haben einen Brief an einige der größten Werbetreibenden geschickt, in dem sie aufgefordert werden alle persönlichen Daten zu löschen, die sie mittels europäischer Cookie-Banner gesammelt haben – andernfalls drohten Schadensersatzforderungen. Zudem sollen die Konzerne aufhören in den USA Cookie-Banner einzusetzen, die die Autoren des Briefes als „Consent Spam" klassifizieren. Zu den Empfängern dieser Forderung gehören die Unternehmen Procter & Gamble und Unilever, aber auch IBM, Mastercard und Ford.

Die IAB ruft unterdessen die europäischen Datenschutzbehörden dazu auf öffentlich ihre Position zu unterstützen und zu erklären, dass sie nicht vorhaben gegen irgendjemanden Maßnahmen zu ergreifen, der weiterhin das TCF-System verwendet. Dass diese Forderung erfüllt wird, ist jedoch sehr unwahrscheinlich. Die niederländische Aufsichtsbehörde hat bereits zuvor dazu aufgerufen das Nutzertracking einzustellen und alternative Methoden der Werbeausspielung zu suchen. Deutsche Behörden haben sich in der Vergangenheit abwartender gezeigt als viele ihrer europäischen Kollegen, aber auch sie haben an dem Beschluss der belgischen Kollegen mitgewirkt. Wann sie zu Zwangsmitteln wie Bußgeldern greifen wollen, lässt sich heute jedoch noch nicht absehen (Kleinz, Belgische Datenschutzaufsicht: Zentraler Standard für Cookie-Banner rechtswidrig, www.heise.de 02.02.2022, Kurzlink: https://heise.de/-6346178; Kleinz, Cookie-Banner: IAB Europe klagt gegen Datenschutz-Entscheidung, www.heise.de Kurzlink: https://heise.de/-6447152).

Frankreich/EU

CNIL erklärt Google Analytics für rechtswidrig

Die französische Datenschutzbehörde Commission Nationale de l'Informatique et des Libertés (CNIL) hat entschieden, dass der Einsatz von Google Analytics auf Webseiten mit europäischen Besuchern nicht mit der Datenschutz-Grundverordnung (DSGVO) vereinbar ist. Wer das Statistikprogramm nutze, verstoße gegen die Vorgaben des Gesetzes zur Datenübermittlung. Google habe für den Transfer in die USA zwar zusätzliche Schutzmaßnahmen ergriffen. Diese reichten aber nicht aus, „um den Zugriff auf diese Daten durch US-Geheimdienste auszuschließen". Mitte Januar 2022 hatte die österreichische Datenschutzbehörde (DSB) einen ähnlichen Beschluss gefasst. Hintergrund ist das „Schrems-II"-Urteil des Europäischen Gerichtshofs (EuGH) vom Sommer 2020, mit dem dieser den transatlantischen „Privacy Shield" und damit eine der wichtigsten Grundlagen für den Transfer von Kundendaten in die USA für ungültig erklärte. Die Luxemburger Richter monierten, dass US-Gesetze wie der Cloud Act eine Massenüberwachung ermöglichten und die Datenschutzstandards nicht vergleichbar seien (DANA 3/2020, 199 ff.).

Max Schrems und der von dem Juristen gegründete Datenschutzverein noyb reichten daraufhin 101 Musterbeschwerden in fast allen EU-Staaten ein. Die CNIL wies nun den Betreiber einer betroffenen französischen Webseite an die darüber erfolgende Datenverarbeitung mit der DSGVO in Einklang zu bringen. Er müsse daher „gegebenenfalls die Nutzung der Google-Analytics-Funktionalität" unter den derzeitigen Bedingungen einstellen und innerhalb von einem Monat auf ein Werkzeug setzen, das keine persönlichen Informationen in die USA übertrage.

Die von Schrems angeführten französischen Unternehmen, die zum Zeitpunkt der Beschwerden Google Analytics verwendeten, waren die Einzelhändler Auchan und Decathlon sowie das Kosmetikgeschäft Sephora. Die Eingabe von noyb richtete sich zudem in Frankreich etwa gegen das Online-Magazin HuffPost, das Facebook Connect nutzt. Die Untersuchung der CNIL und ihrer europäischen Partner erstreckt sich auch auf solche Instrumente, mit denen ebenfalls Daten europäischer Nutzer in die USA gelangen. Einschlägige Entscheidungen sollen bald folgen. Auch die niederländische Datenschutzbehörde hat einen Beschluss gegen Google Analytics angekündigt. Zum Messen und Analysieren der Besucherzahlen einer Webseite empfiehlt die CNIL Dienste, die mit anonymen statistischen Daten arbeiten. Hier könne eine Ausnahme von der prinzipiell erforderlichen Einwilligungspflicht greifen, wenn sicherge-

stellt werde, „dass keine illegalen Übermittlungen stattfinden“. Google mahnt derweil nachdrücklich einen Privacy Shield-Nachfolger an (Krempl, Frankreichs Datenschutzbehörde: Google Analytics ist in der EU rechtswidrig, www.heise.de 10.02.2022, Kurzlink: https://heise.de/-6439306).

EU/Irland

Erneutes Bußgeld gegen Meta

Die Datenschutzaufsichtsbehörden der EU-Mitgliedsländer haben unter Federführung der irischen Datenschutzbehörde Meta Platforms zur Zahlung eines Bußgeldes in Höhe von 17 Millionen Euro verpflichtet. Als Begründung werden insgesamt zwölf Verletzungen von Datenschutzrecht durch den Facebook-Betreiber angeführt, die 2018 beanstandet wurden. Da der EU-Hauptsitz der Social-Media-Plattform in Irland liegt, leitet die irische Aufsichtsbehörde, die Datenschutzkommission (DPC), das Verfahren. Die DPC hat festgestellt, dass Meta beziehungsweise Facebook „keine angemessenen technischen und organisatorischen Maßnahmen“ getroffen habe, um Daten von EU-Nutzern zu schützen. Meta vertritt den Standpunkt, dass Facebook lediglich gegen Dokumentationspflichten verstoßen habe. Die internen Abläufe würden weiterentwickelt.

2021 hatte die irische Datenschutzbehörde WhatsApp, eine weitere Meta-Tochter, mit einem Bußgeld in Höhe von 225 Mio. Euro belegt. Grund für das höchste Bußgeld, das sie je verhängte, war der Verstoß gegen die Datenschutz-Grundverordnung (DSGVO), wonach WhatsApp seinen Transparenzverpflichtungen in Bezug auf die Bereitstellung von Informationen und deren Weiterverarbeitung zwischen WhatsApp und anderen Meta-Unternehmen nicht nachgekommen sei. Zuletzt hat Meta vor möglichen Konsequenzen gewarnt, sollten die Verhandlungen über Transfers europäischer Daten in die USA keine Früchte tragen. Ohne Datentransfer, so der Jahresbericht des US-Konzerns, müssten sie Facebook und Instagram in der EU abschalten (Schräer, Datenschutzverletzungen: Irland verhängt 17 Millionen Euro Bußgeld gegen Meta, www.heise.de 16.03.2022, Kurzlink: https://heise.de/-6550578).

Schweiz

Verdacht russischer Spionage gegen SMS-Dienst Mitto

Twitter und andere Unternehmen kappen die Geschäftsbeziehungen zu dem Schweizer Unternehmen Mitto AG, das massenhaft SMS verschicken kann, aber nebenher und heimlich die Überwachung von Mobilfunkgeräten ermöglicht hat. Man sei dabei für den Versand von Verifikations-PINs zu anderen Dienstleistern zu wechseln, erklärte Twitter gegenüber dem US-Senator Ron Wyden (Demokraten).

Die geheimen Nebengeschäfte von Mitto waren im Dezember 2021 bekannt geworden. Die zunächst vom Bureau of Investigative Journalism und von Bloomberg erhobenen Vorwürfe richten sich hauptsächlich gegen den Mitgründer von Mitto, Ilja Gorelik. Mitto hat Verträge mit Providern in aller Welt, um SMS in großen Mengen und auch in schwer erreichbare Staaten wie etwa Afghanistan und den Iran zu schicken. Dafür zahlen nicht nur IT-Riesen wie Google, WhatsApp, Microsoft und eben Twitter, die über Mitto etwa SMS mit Verifikationsnummern verschicken. Den Recherchen zufolge verkaufte er die Zugänge zu den Mobilfunknetzen an Kunden, die das z.B. für die Standortüberwachung von Mobilfunkgeräten nutzen konnten. Dazu habe er eigenmächtig Software installiert. Kunden, Provider und angeblich sogar Mitto selbst hätten davon nichts gewusst. Der Schweizer Datenschutzbeauftragte ermittelt.

Wenige Tage nach den Berichten über diese geheimen Nebengeschäfte und fragwürdige Praktiken im Unternehmen selbst hatte eine Schweizer Tageszeitung Geschäftsverbindungen nach Russland aufgedeckt. Mitto ist demnach hundertprozentige Mutter einer mutmaßlichen Briefkastenfirma in Moskau, die in dem Jahr gegründet wurde, in dem die heimlichen Überwachungsaktivitäten ihren Ausgang genommen haben. Für den Geheimdienstexperten Erich Schmidt-Eenboom weckte die Enthüllung den Verdacht, „dass russische Dienste mit Informationen von Mitto versorgt worden sein könnten“. Mitto selbst hatte angesichts der ersten Enthüllungen eine interne Untersuchung eingeleitet (Holland, Geheime Spionagegeschäfte: Twitter trennt sich von Schweizer SMS-Firma, www.heise.de 10.02.2022, Kurzlink: https://heise.de/-6368789).

Italien

Bologna plant ein Social Credit System

In Bologna wird derzeit das erste europäische Sozialkreditsystem entwickelt. Unter dem Namen „Smart Citizen Wallet“ sollen Italiener für Wohlverhalten wie Mülltrennung und Nutzung öffentlicher Verkehrsmittel Punkte sammeln können, indem sie mittels einer App auf dem Mobiltelefon ab Herbst 2022 Tugendpunkte sammeln können. Wer nachweislich den Müll getrennt oder öffentliche Verkehrsmittel benutzt hat und nie im Parkverbot stand, erhält Gutschriften. In was sie umgetauscht werden können, also die Belohnung, steht noch nicht fest.

China arbeitet seit 2014 in Testregionen mit einem solchen System an der Verhaltenssteuerung der Bevölkerung. Wer sich wohl verhält, erlangt dort leichteren Zugang zu Krediten und Visa, wer negativ auffällt, muss mit Reisebeschränkungen und Steuererhöhungen rechnen. Dabei werden Technologien optischer Überwachung ebenso eingesetzt wie die Auswertung der Datenmengen, die das Smartphone liefert, wenn mit ihm gebucht und bezahlt wird.

Die europäische Variante, die bei Freiwilligkeit der Teilnahme einstweilen nur positive Sanktionen vorsieht, verwandelt das öffentliche Leben und seine Probleme eher in ein Spiel. Die italienische Autorengruppe „Ippolita“ hat das in ihrem Buch über „Elektrische Seelen“ („Anime elettriche“, 2016) analysiert. Es werden danach moralische Rabattmarken verteilt, die den Zugang zu Gütern und Konsumlevels eröffnen, je nachdem, wie viele Punkte gesammelt wurden. Die Gesellschaft verwandelt sich dort, wo die Tugendabrechnung etabliert wird, in eine Organisation.

Im idealen Fall werden überall Messstationen eingerichtet, die den Gehor-

sam ermitteln, und die digitalen Personalakten wachsen. Es muss festgelegt werden, was erwünscht ist und wie viel dafür zurückgezahlt werden kann, damit das Erwünschte geschieht. Die Abweichungen davon, Ungehorsam, Indifferenz und Eigensinn, gelten als unsozial. Was getan wird, wird aufgrund einer erwartbaren Auszahlung getan. Zugleich ist aus China der Begriff der „unsichtbaren roten Linie" bekannt, der die Ungewissheit darüber bezeichnet, was denn genau sozial erwünscht ist und ob verlangtes Verhalten nicht stets auch Schattenseiten hat.

Konformismus ist nicht einfach, zumal in der Gesellschaft seit jeher ganz unterschiedliche Normen gelten, deren jeweilige Befolgung nur zufällig zueinander passt. Wenn die Leute nachts an unbefahrenen Straßen rote Fußgängerampeln beachten, so der FAZ-Kommentator Kaube, können sie sowohl ein Lob des regelgerechten Handelns erwarten wie die Beschreibung, kadavergehorsam und also willenlos zu sein. Deviant sind die Verbrecher wie die Rebellen, die Erfinder wie die Melancholiker. Aus dieser Vielfalt der Abweichungen von den Pfaden der Tugend lebt jedes Gemeinwesen. Wenn uns also jemand fragte, wohin Europa geht, sollten wir eher nicht sagen „nach Bologna" (Kaube, Tugendpunkte in Bologna. www.faz.net 21.04.2022).

Ukraine

Mit Clearview getötete Soldaten identifizieren

Die Ukraine verwendet nach eigenen Angaben die Gesichtserkennungssoftware der umstrittenen US-Firma Clearview AI, um russische im Ukrainekrieg getötete Soldaten zu identifizieren. Die Ukraine wolle dann die betroffenen Familien über den Tod ihrer Angehörigen informieren, erklärte der Vizepremierminister und Minister für die digitale Transformation, Mykhailo Fedorov. Das ukrainische Verteidigungsministerium habe im März 2022 mit der Nutzung begonnen. Mit der auf künstlicher Intelligenz basierenden Mustererkennung von Clearview sollen die Social-Media-Konten der verstorbenen Soldaten gefunden werden.

Das ukrainische Innenministerium unterhält einem Reuters-Bericht zufolge einen Telegramkanal „Look for your own", auf dem Bilder von nicht identifizierten gefangenen oder getöteten russischen Soldaten veröffentlicht werden, damit Verwandte sich melden können. Nach Angaben des ukrainischen Militärs waren seit Kriegsbeginn am 24.02.2022 bis zum 24.03. etwa 15.000 russische Soldaten getötet worden.

Pathologen der US-Armee erklärten, dass die automatische Gesichtserkennung derzeit noch keine akzeptierte Methode sei, um Leichen zu identifizieren. Der Leiter der Abteilung für forensische Medizin an der Monash University in Melbourne, Richard Bassed, meinte, „trübe Augen und verletzte, ausdruckslose Gesichter" würden die Gesichtserkennung bei Verstorbenen unzuverlässig machen. Clearview soll seinen Dienst der Ukraine nach der russischen Invasion kostenlos angeboten haben. Die Datenbank enthalte über zwei Milliarden Bilder von VKontakte, einem beliebten russischen Social-Media-Dienst (zu Clearview DANA 1/2022, 45, 54 f.; Koch, Gesichtserkennung: Ukraine setzt Clearview AI zur Identifizierung Gefallener ein, www.heise.de 24.03.2022, Kurzlink: https://heise.de/-6624818).

Russland

Nokia förderte telekommunikative Sorm-Überwachung

Nach dem russischen Angriff auf die Ukraine hat der finnische Konzern Nokia seine Lieferungen nach Russland eingestellt. Zuvor soll er allerdings beim Ausbau eines umfangreichen Überwachungssystems innerhalb des Landes geholfen haben. Gemäß der „New York Times" ergibt sich aus internen Unternehmensdokumenten, dass Nokia dem größten russischen Mobilfunkanbieter MTS sowohl Hard- als auch Software zur Verfügung gestellt hat, die für die Überwachung russischer Bürgerinnen und Bürger von Bedeutung ist. Bei der Recherche sollen mehr als 75.000 Dokumente und fast 2 Terabyte Datensätze ausgewertet worden sein. Die Vorwürfe hängen mit dem System for Operative Investigative Activities, kurz Sorm, zusammen. Damit hört der russische Inlandsgeheimdienst FSB nicht nur Telefongespräche ab, sondern fängt auch E-Mails sowie Textnachrichten ab und verfolgt die Internetkommunikation der Menschen.

Nokia habe, so der Bericht, zwar keine Technologie hergestellt, um direkt die Kommunikation abzuhören. Allerdings habe der Konzern mit staatsnahen russischen Unternehmen zusammengearbeitet, um die Verbindung des Sorm-Systems mit dem Netzwerk von MTS zu planen, zu optimieren und Fehler zu beheben. Dies sei besonders brisant vor dem Hintergrund, dass Sorm offenbar auch in Russland eingesetzt wird, um Gegner des Kriegs zum Schweigen zu bringen. Die Dokumente sollen zeigen, „dass Nokia wusste, dass es ein russisches Überwachungssystem ermöglichte". Diese Arbeit sei für Nokia unerlässlich gewesen, um in Russland Geschäfte zu machen, nachdem das Unternehmen zu einem der wichtigsten Lieferanten von Geräten und Dienstleistungen für verschiedene Telekommunikationskunden geworden war. Sie spülten jährlich Hunderte von Millionen Dollar in die Kasse des Konzerns, „selbst als Putin im Ausland immer kriegerischer und im Inland immer kontrollsüchtiger wurde". Es wird davon ausgegangen, dass Putin Kritiker seines Ukrainekrieges per Sorm verfolgen lässt. Zuvor hatte Sorm geholfen, Anhänger des Oppositionellen Alexej Nawalny ausfindig zu machen.

Nokia bestritt die Echtheit der Dokumente nicht und rechtfertigte sich damit, „dass es nach russischem Recht verpflichtet sei Produkte herzustellen, die es einem russischen Telekommunikationsbetreiber ermöglichen sich mit dem Sorm-System zu verbinden". Andere Länder würden ähnliche Forderungen stellen. Nokia erklärte, dass es selbst „keine Sorm-Geräte herstellt, installiert oder wartet". Nach dem Angriff Russlands auf die Ukraine hatte der finnische Konzern diesen scharf verurteilt, seine Lieferungen nach Russland eingestellt und sich aus dem Russlandgeschäft zurückgezogen. Die Hinterlassenschaft des Konzerns bleibt in Betrieb.

Der russische Geheimdienstexperte Andrej Soldatow vom Center for European Policy Analysis in Washington

meinte, ohne Nokias Hilfestellung bei der Integration von Sorm in das MTS-Netzwerk „wäre es nicht möglich gewesen so ein System aufzubauen“. Tom Malinowski, demokratischer Abgeordneter im US-Repräsentantenhaus, forderte Konsequenzen. Umfassendere Exportkontrollen für westliche Technologien sollten verhindern, dass diese für die Totalüberwachung der Bürger eingesetzt werden können. Mit diesen Produkten solle nicht anders verfahren werden als „mit fortschrittlicher Raketen- oder Drohnentechnik“ (Ist Nokia für die Überwachung von Putin-Gegnern in Russland verantwortlich? www.mdr.de 29.03.2022; Nokia assistierte bei Putins Spitzelei, Der Spiegel Nr. 14 v. 02.04.2022, 95).

Russland

Yandex-Food-Daten enttarnen Geheimdienstmitarbeiter

Wegen eines Datenlecks beim Essenslieferdienst Yandex Food, das am 01.03.2022 bekannt wurde, weiß die Welt, was und wo einige Russen essen, auch solche, die gern möglichst geheim leben. Die russische Medienaufsichtsbehörde Roskomnadsor hat noch versucht die Daten wieder einzufangen. Sie hat mit Strafen gedroht, hat eine Website gesperrt; geholfen hat es letztlich nicht.

Die Journalisten des Investigativportals Bellingcat haben den Datensatz ausgewertet. Dabei gelang es ihnen unter anderem ein Gebäude und mehrere Personen dem russischen Geheimdienst zuzuordnen. Dass das über scheinbar nebensächliche Daten gelang – wer hat welches Essen wohin bestellt? –, zeigt, dass es keine harmlosen Daten gibt. Verbindet man die Datenpunkte, dann können sie Geheimnisse enthüllen: Die Journalisten ordneten die Daten Informationen zu, die sie bereits hatten, teils aus anderen Leaks. Sie überprüften beispielsweise, welche Lieferungen an die Adresse Doroschnaja Straße 56 in Moskau gingen. Das dortige Gebäude wird der russischen Nationalgarde zugeordnet. Oder an die Choroschowskoje Chaussee 76, das Hauptquartier des Militärgeheimdienstes GRU.

Die Bestellungen enthielten auch Handynummern. Die Reporter verglichen sie mit den Nummern, die sie bei einer Recherche zu den Beteiligten des Mordkomplotts gegen den inzwischen inhaftierten Oppositionellen Alexej Nawalny erhalten hatten. Ein neuer Name tauchte dabei auf. In der Nacht des Anschlages telefonierten die mit der Vergiftung Nawalnys betrauten FSB-Offiziere demzufolge mehrfach mit jemandem bei einem Forschungsinstitut in Dubna, einer Stadt in der Oblast Moskau. Dieser Mann bestellte irgendwann Essen. Er gab dabei seinen Namen samt Handynummer an.

In dem Leak taucht auch Putins angebliche „geheime Tochter“ auf, die er mit der ehemaligen Putzkraft – und heutigen Besitzerin einer Luxuswohnung in Monaco – Swetlana Kriwonogich haben soll. Sie bestellte Essen in ein rund 400 Quadratmeter großes Apartment, das umgerechnet etwa zwei Millionen Euro wert sein soll. Ljubow Sobol, eine russische Juristin und Oppositionspolitikerin, hatte darüber auf Twitter berichtet. Über andere Namen, die für die Öffentlichkeit weniger interessant sind, berichtete Bellingcat nicht. Der eigentliche Datensatz, der überwiegend Informationen zu den Bestellungen unbekannter russischer Bürger enthält, sei „ohne legitimes Interesse für die Forschung“ und daher nicht Teil der Publikation.

Das Leak reiht sich in mehrere schwere Pannen ein, bei denen die Daten zahlreicher Russen abflossen. In einer anderen Recherche schrieb Bellingcat, um an Informationen über russische Bürger zu kommen – etwa zu ihren Bewegungen anhand von Handydaten, zu ihrem Wohnsitz, zu ihrem Reiseverhalten und ihren Telefonaten –, brauche es nicht mehr „als ein bisschen kreatives Googeln (oder Yandexen) und ein paar Hundert Euro in Kryptowährungen“. Yandex ist die russische Alternative zu Google.

Der Grund für die einfache Zugänglichkeit solcher Daten ist die Sammelwut russischer Behörden, die gern alles über ihre Bürgerinnen und Bürger wissen wollen. Die örtlichen Telekommunikationsunternehmen müssen seit 2016 Kundendaten speichern. So entstehen lohnende Ziele für Hacker. Zudem verkaufen die Unternehmen diese Daten oft heimlich weiter. All das Sammeln und Speichern macht den russischen Staatsapparat also – zumindest in diesem Fall – nicht sicherer, sondern vielmehr angreifbarer. Sicherheitsforscher Troy Hunt wies darauf hin, dass jeder irgendwann in einem Leak landen kann. Das Yandex-Food-Leak soll Informationen zu knapp 60 000 Russen enthalten. 2019 flossen die Daten von 4,9 Millionen Kunden des US-Lieferdienstes Doordash ab (Bovermann, Lieferdienst-Datenleck enttarnt russische Geheimdienstmitarbeiter, SZ 06.04.2022, 18).

Israel

Pegasus erschüttert israelische Politik

Die israelische Wirtschaftszeitung „Calcalist“ veröffentlichte Anfang Februar 2022 eine lange Liste von Zielpersonen, die von der israelischen Polizei illegal mit der von der Firma NSO entwickelten Spionagesoftware Pegasus ausgespäht worden sein sollen. Bürgermeister sind darunter, Wirtschaftsführer, hohe Staatsbeamte sowie viele Personen aus dem engsten Umfeld des früheren Premierministers Benjamin Netanjahu, darunter sein Sohn Avner. Mit dieser Enthüllung schlug der NSO-Skandal mit einiger Verspätung auch in Israel, an der Quelle, hohe Wellen. NSO ist eine israelische Firma, deren Späh-Software unbemerkt die Kontrolle über Mobiltelefone übernehmen kann. Der damit mögliche Missbrauch stand im Mittelpunkt des sogenannten „Pegasus-Projekts“, bei dem internationale Medien im Sommer 2021 aufdeckten, wie autoritäre Regime weltweit Journalisten, Menschenrechtler und Oppositionelle ausspähen (DANA 3/2021, 187 ff).

In den USA wurde die Firma NSO inzwischen auf eine Sanktionsliste gesetzt. In Israel aber hatte sie sich bis dahin der Protektion durch die Politik sicher sein dürfen. Zu den Beschwichtigungsformeln der Software-Entwickler zählte unter anderem die Behauptung, dass ihre Produkte nur zur Bekämpfung von Terrorismus und organisierter Kriminalität eingesetzt würden und dass israelische ebenso wie US-amerikanische Telefonnummern gar nicht ausge-

späht werden könnten – was nun offenbar widerlegt wurde.

Auf die ersten Anschuldigungen hin hatte Israels Polizei noch mit einem erbosten und kategorischen Dementi reagiert. Zweiflern wurde vorgehalten, sie würden die Arbeit der Polizei behindern und das Land den Verbrechern und Terroristen überlassen wollen. Zwei Wochen später wurde dann allerdings vage einräumt, es gebe „neue Erkenntnisse". Am 07.02.2022 wurden auf der Liste Ross und Reiter genannt mit den Namen Dutzender Personen, deren Telefone ohne Verdacht auf kriminelle Handlungen und ohne richterliche Genehmigung von der Polizei gehackt worden sein sollen. Es findet sich darauf zum Beispiel Rami Levy, der landesweit bekannte Besitzer einer großen Supermarktkette. Auch die drei Generaldirektoren der Ministerien für Finanzen, Justiz und Transport stehen darauf, offenbar wegen des Verdachts der Weitergabe von Informationen an Journalisten. Die Anführer von Protestbewegungen wurden demnach ebenso ausgespäht wie Siedlervertreter vor geplanten Räumungsaktionen. Das alles wirkte recht wahllos und vor allem: unkontrolliert.

Die Innenministerin Ayelet Schaked zeigte sich irritiert: „Wenn diese Berichte stimmen, dann sprechen wir von einem Erdbeben und von Taten, die zu dunklen Regimen aus früheren Jahrhunderten passen". Schaked galt bislang als enge Freundin der NSO-Präsidentin Schiri Dolev. Auch Premierminister Naftali Bennett hatte zu Beginn der Corona-Pandemie vor zwei Jahren noch eine Software von NSO zum Tracking bei der Corona-Bekämpfung einsetzen wollen. Nun versprach er der Bevölkerung volle Aufklärung über den möglichen Missbrauch: „Wir verstehen den Ernst dieser Angelegenheit." Sogar Israels Präsident Isaac Herzog schaltete sich ein: „Wer für Recht und Ordnung sorgt, muss sauberer als alle anderen sein. Wir dürfen nicht unsere Demokratie und das Vertrauen in unsere Polizei verlieren."

Den lautesten Alarm schlug der frühere Premier und heutige Oppositionsführer Benjamin Netanjahu, indem er von einem „dunklen Tag für den Staat Israel" sprach. Ein solcher Einsatz der Spähsoftware sei vergleichbar damit, dass Israels Armee die eigenen Bürger bombardiere. Es war Netanjahu persönlich, der den Polizeichef Roni Alscheich ausgewählt hatte, in dessen Amtszeit von 2015 bis 2018 offenbar die meisten Ausspähungen fielen. Alscheich war zuvor Vize beim Inlandsgeheimdienst Schin Bet gewesen, und Netanjahu gab ihm den Auftrag mit auf den Weg, die Cybertechnologie in die Polizeiarbeit einzubringen. Vor allem aber hatte Netanjahu selbst die NSO-Spionagesoftware weltweit angepriesen. Seine „Pegasus-Diplomatie" mit dem Verkauf der israelischen Software soll zum Beispiel dabei geholfen haben den Weg zur Aufnahme diplomatischer Beziehungen zu mehreren arabischen Staaten zu ebnen.

Netanjahu sieht jetzt die Chance den Skandal in seinem Korruptionsprozess zu nutzen. Denn auf der Liste jener, die von der Polizei illegal gehackt worden sein sollen, stehen zahlreiche Personen aus seinem engeren Umfeld, diverse wichtige Zeugen sowie andere Angeklagte. Seine Anwälte erhoffen ein Ende des Verfahrens. Zumindest sollen die Anhörungen erst einmal eingestellt werden. Klarheit über den israelischen Pegasus-Einsatz wird es aber nicht kurzfristig, allenfalls in einigen Monaten geben. Der zuständige Minister für die öffentliche Sicherheit hat die Einsetzung einer Untersuchungskommission angekündigt (Münch, Neuer Abhörskandal erschüttert Israel, SZ 09.02.2022, 7).

USA

Clearview wirbt mit Expansion bei der Gesichtserkennung

Trotz zahlreicher rechtlicher Verfahren und internationaler Kritik expandiert die auf biometrische Gesichtserkennung spezialisierte US-Firma Clearview (s.o. S. 117). Das Unternehmen sei, so eine 55-seitige Präsentation für Investoren von Clearview, dabei die Zahl der in seiner Datenbank gespeicherten Gesichtsfotos binnen eines Jahres von 10 Milliarden auf 100 Milliarden zu erhöhen. Dies dürfte gewährleisten, dass „fast jeder Mensch auf der Welt identifizierbar sein wird". Die New Yorker Firma hätte damit durchschnittlich 14 Fotos von jedem der 7 Milliarden Erdenbürger in ihrem Register, mit dem sie derzeit Erkennungsdienste für Sicherheitsbehörden weltweit durchführt. Das jährliche Wachstum der Datenbank gibt das Unternehmen aktuell mit 1,5 Milliarden Bildern pro Monat an. Bei dieser Rate müsste es noch deutlich zulegen, denn sonst kämen innerhalb eines Jahres „nur" 18 Milliarden Bilder dazu.

50 Millionen US-Dollar will Clearview dem zugrundeliegenden Pressebericht zufolge von Investoren einwerben, um schneller zu wachsen und in neue Geschäftsfelder vorzustoßen. Die Firma betonte nach außen bislang immer, nur mit Regierungsstellen und insbesondere mit Strafverfolgern zusammenzuarbeiten. Nun behauptet sie in der Präsentation die Art und Weise „revolutionieren" zu können, wie Arbeitskräfte in der Gig Economy überprüft werden. Daneben sollen sich Logos etwa von Airbnb, Lyft und Uber befinden.

Clearview-Gründer Hoan Ton-That bezeichnete diese Namen gegenüber der Zeitung als „Beispiele für die Art von Unternehmen, die Interesse an der Gesichtserkennungstechnologie" der Firma „zum Zwecke der zustimmungsbasierten Identitätsüberprüfung bekundet haben". Sie wollten damit verhindern, dass über ihre Plattformen Straftaten begangen würden. Sprecher der genannten Konzerne betonten noch nie Pläne für eine Zusammenarbeit gehabt zu haben. Ferner soll Clearview damit werben, dass die biometrische Erkennungstechnik dazu verwendet werden könnte, um Menschen auf Apps zu bewerten, über die Nutzer etwa nach Partnern, Babysittern, Reinigungskräften oder Handwerkern suchten. Auch die Betreiber von Anwendungen wie Tinder, Sittercity & Co. wollten davon aber nichts wissen und monierten, dass Clearview ihre Logos missbrauche.

Das Unternehmen gibt dem Bericht nach zudem an, dass es neben der Gesichtserkennung andere Systeme etwa zum Scannen von Nummernschildern und zur „Bewegungsverfolgung" entwickelt habe. Es arbeite zudem nach eigenen Angaben an einer Reihe anderer automatisierter Überwachungstechniken. Darunter befinde sich Kamerasoftware zur Erkennung von Waffen und Drogen, Systeme zur Identifizierung einer

Person anhand ihres Gangs und „Image to Location"-Programme zur Bestimmung des Aufenthaltsorts einer Person anhand des Hintergrunds eines Fotos. Ferner verweise es auf eine Software, um eine Person aus der Ferne anhand einer Aufnahme ihres Fingerabdrucks zu identifizieren. Ton-That erklärte, diese Techniken dienten alle der öffentlichen Sicherheit und befänden sich in verschiedenen Stadien der Forschung und Entwicklung. Sie seien noch nicht marktreif und noch nicht in der Praxis eingesetzt worden.

Die Präsentation widerspricht einem offenen Brief von Clearview aus dem Januar 2022, wonach man auf eine Echtzeiterkennung bewusst verzichte, um die Menschenrechte und Grundfreiheiten zu schützen. Zusammen mit Behörden soll laut den Informationen für Geldgeber doch ein „Echtzeit-Warnsystem" entstehen. Damit könnten Unternehmen die Polizei benachrichtigen, wenn sie etwa „Personen mit hohem Risiko" entdecken. Bereits bekannt war, dass die Firma für die US-Luftwaffe ein Pilotprojekt für eine Datenbrille mit Augmented-Reality-Gesichtserkennung durchführen soll.

Amazon, Google, IBM und Microsoft haben sich aus dem Markt für Gesichtserkennungssysteme weitgehend zurückgezogen. Kritiker warnen, die Technik sei unzuverlässig, fehleranfällig und könnte leicht missbraucht werden. Clearview sieht im eigenen Kurs dagegen beste Geschäftsmöglichkeiten, da es in den USA nun nur noch wenig Konkurrenz habe. Sein Stammprodukt sei zudem mächtiger als in China verwendete Lösungen, da das Fotoregister mit „Metadaten aus öffentlichen Quellen" und Informationen aus sozialen Netzwerken verbunden sei. Die Aufnahmen hat die Firma vor allem aus Facebook, Instagram, Twitter & Co. sowie aus privaten Webseiten zusammengesammelt. 2021 warfen die Aufsichtsbehörden in Frankreich, Österreich, Italien, Griechenland und Großbritannien dem Unternehmen vor gegen europäische Datenschutzgesetze zu verstoßen. Bereits ergangenen Löschaufforderungen sollen teils Geldbußen folgen. In den USA laufen in mehreren Bundesstaaten Klagen gegen Clearview (Krempl, Überwachung: Clearview will Datenbank mit 100 Milliarden Gesichtsfotos füllen, www.heise.de 17.02.2022, Kurzlink: https://heise.de/-6491056).

USA

Vergleich wegen Werbenutzung der Facebook-Like-Daten auf Fremdseiten

Vor dem US-Bundesbezirksgericht für Nordkalifornien wurde ein Vergleich zur Genehmigung vorgelegt, wonach Facebook 90 Millionen Dollar zahlen soll, um eine Sammelklage abzuwenden, die bereits im Jahr 2012 gegen den Konzern eingereicht worden war (Az. 12-md-02314). Als Facebook im Jahr 2010 die Funktion des Like-Buttons auf anderen Webseiten einführte, sollte gemäß dem Konzern den Nutzenden die Möglichkeit gegeben werden ihre Vorlieben zu äußern. Aus den Gerichtsunterlagen ging allerdings hervor, dass die Funktionalität des Buttons deutlich weiter geht. Mithilfe von Cookies wurden so Nutzerdaten gesammelt, unter anderem Informationen darüber, welche Webseiten besucht wurden, welche Artikel angesehen wurden, oder welche Produkte gekauft wurden. Diese Daten wurden unabhängig davon erhoben, ob der Like-Button vom Webseitenbesucher genutzt wurde, oder ob der Nutzer noch bei Facebook eingeloggt war. Das wurde vonseiten Facebooks zunächst bestritten.

Der Computer-Experte Nik Cubrilovic wies jedoch nach, dass Daten auch von ausgeloggten Nutzern erhoben wurden. Daraufhin räumte das Unternehmen Fehler ein und sah von der Datenerhebung bei ausgeloggten Nutzern künftig ab. Der daraus resultierende Rechtsstreit zog sich über Jahre hin. 2017 gelang es Facebook die Verfahren einstellen zu lassen. Doch das hat ein Bundesberufungsgericht 2020 wieder aufgehoben. Statt der ursprünglich geforderten Dutzenden Milliarden Dollar dürfte der Facebook-Konzern Meta Platforms mit 90 Millionen US-Dollar Entschädigungszahlungen davonkommen gemäß dem Vergleich, auf den sich Facebook und die Kläger geeinigt haben. Ausgehandelt wurde er mit Hilfe eines Mediators. Das beobachtete Nutzungsverhalten konnte Facebook in höhere Einnahmen von Werbekunden ummünzen. Der Datenkonzern gibt an mit den im erwähnten Zeitraum gesammelten Daten nicht mehr als die nun gebotenen 90 Millionen Dollar verdient zu haben. Die damals gesammelten Daten würden bei Genehmigung des Vergleichs gelöscht, verspricht Meta.

Von den 90 Millionen Dollar geht ein Brocken an die Anwälte der Kläger. Da hier mindestens 21 Klagen zusammengefasst sind, und die jeweiligen Anwälte seit 2011/2012 an dem Verfahren arbeiten, kommt einiges zusammen. Die Juristen haben insgesamt rund 26 Millionen Dollar Honorare zuzüglich Auslagen angemeldet. Auch die Verwaltung des Fonds sowie Druck und Versand der Entschädigungsschecks kostet. Der Rest kann unter den geschätzt 126 Millionen US-Amerikaner verteilt werden, die Facebook im Zeitraum 22. April 2010 bis 26. September 2011 genutzt haben.

In seinem Antrag an das Gericht verweist Meta auf eine Statistik der US-Handelsbehörde FTC (Federal Trade Commission), wonach bei über 100 erfolgreichen US-Sammelklagen im Median nur 4-5% der Berechtigten einen Antrag auf Auszahlung gestellt haben. Außerdem erwähnt Meta einen Rechtsprofessor, der herausgefunden habe, dass die Antragsrate bei sehr großen Sammelklagen (mehr als 2,7 Millionen Berechtigte) unter 1,5% liegt. Sollten nach Abzug der Anwaltshonorare und aller anderer Kosten 54 Millionen Dollar im Topf bleiben, und sich ein Prozent der Berechtigten anmelden, könnte jeder gut 42 US-Dollar bekommen (entspricht 37 €). Je mehr ihre Auszahlung fordern, desto weniger bekommt jeder.

Auch in Europa wurde die Facebook-Praxis kritisiert. Der Europäische Gerichtshof (EuGH) hat in einem Urteil im Jahr 2019 festgestellt, dass Seitenbetreiber mitverantwortlich für die Datenverarbeitung sein können. Im aktuellen Fall gilt der Vergleich für US-amerikanische Facebook-Nutzende, die zwischen April 2010 und September 2011 ein Facebook-Konto besaßen und andere Webseiten besuchten, auf denen der Like-Button eingesetzt wurde. Die Entscheidung des Gerichts zu dem Vergleichsvorschlag steht noch aus (Hillnhütter, 90 Millionen Dollar wegen Facebook-

Like-Button, www.onlinehaendler-news.de 16.02.2022; Sokolov, Facebook bietet 90 Millionen Dollar Entschädigung für heimliches User-Tracking, www.heise.de 16.02.2022, Kurzlink: https://heise.de/-6477298).

USA

Diskriminierende Videoüberwachung mit Gesichtserkennung in New York

Im April 2021 begannen über 7.000 Freiwillige im Rahmen des Projekts „Decode Surveillance" (Aufdeckung von Überwachung) für Amnesty International (AI) die Standorte von Kameras in den Straßen von New York City mit Hilfe von Google Street View zu dokumentieren. Sie überprüften 45.000 Kreuzungen jeweils dreimal und identifizierten über 25.500 Kameras. Gemäß dem AI-Bericht sind schätzungsweise 3.300 dieser Kameras in öffentlichem Besitz und werden von Behörden und Strafverfolgung genutzt. Das Projekt wurde unterstützt von der Nichtregierungs-Organisation BetaNYC, die unter anderem die Nutzung von Technologie in der Kommunikation zwischen Bürgern und Behörden verbessern will. Zusammen mit Datenwissenschaftlern konnte eine Karte mit den Koordinaten aller 25.500 Kameras erstellt werden. Die Analyse ergab, dass es in den Stadtbezirken Bronx, Brooklyn und Queens am meisten solcher öffentlichen Kameras gibt, also in Regionen mit einer hohen Konzentration von People of Color (PoC).

Um herauszufinden, inwieweit das Kameranetz mit den polizeilichen Durchsuchungen zusammenhängt, ermittelten die AI-Forschenden zusammen mit Datenwissenschaftlern die Häufigkeit der Durchsuchungen pro 1.000 Einwohner im Jahr 2019 in jedem Volkszählungstrakt (geografischer Abschnitt, der kleiner ist als eine Region mit derselben Postleitzahl). Die Grundlage dafür bildeten die von der New Yorker Polizeibehörde NYPD zur Verfügung gestellten Adressdaten. Aus den in dem Bericht zitierten Daten der NYPD geht hervor, dass es in New York seit 2002 mehr als 5 Millionen Mal zu sogenannten „Stop-and-frisk"-Durchsuchungen gekommen ist. Die „Stop-and-frisk"-Methode – das willkürliche Anhalten und Durchsuchen von Menschen auf den Straßen – erlaubt es Beamten stichprobenartige Kontrollen von Bürgern auf Grundlage eines „begründeten Verdachts" durchzuführen. Der größte Teil dieser Durchsuchungen wurde, so ergaben die NYPD-Daten, bei PoC durchgeführt. Nach Angaben der New Yorker Bürgerrechtsorganisation American Civil Liberties Union (ACLU) waren die meisten der durchsuchten Personen unschuldig.

Jedem Volkszählungsgebiet wurde ein „Überwachungslevel" zugewiesen, der sich nach der Anzahl der öffentlichen Kameras pro 1.000 Einwohner richtete. In Gebieten mit hohem Überwachungslevel wurden auch besonders oft Menschen angehalten und durchsucht. Auf einer Strecke von 800 Metern im Brooklyner Stadtteil East Flatbush fanden 2019 beispielsweise sechs derartige Durchsuchungen statt, und die Abdeckung durch öffentliche Kameras lag bei 60%.

Experten befürchten, dass die Strafverfolgungsbehörden die Bilder der Kameras dazu nutzen, um mit Hilfe von Gesichtserkennungs-Technologie unverhältnismäßig viele PoC ins Visier zu nehmen. Auf Anfrage erhielt die Nichtregierungs-Organisation Surveillance Technology Oversight Project (STOP) Dokumente, aus denen hervorgeht, dass die New Yorker Polizei zwischen 2016 und 2019 in mindestens 22.000 Fällen Gesichtserkennung eingesetzt hat, darunter das umstrittene Clearview-System. Matt Mahmoudi von AI kommentierte: „Laut unserer Analyse verstärkt der Einsatz der Gesichtserkennungs-Technologie durch die NYPD die diskriminierende Polizeiarbeit gegen Minderheitengemeinschaften in New York City."

Durch einen Abgleich der Überwachungskarte mit der Marschroute zeigt der Bericht auch auf, wie die Teilnehmer der Black-Lives-Matter-Proteste im Jahr 2021 der Gesichtserkennungstechnologie ausgesetzt waren. Sie wurden laut Mahmoudi „fast vollständig überwacht". Zwar ist nicht genau klar, in welchem Umfang die Gesichtserkennungstechnologie während der Proteste eingesetzt worden ist. Doch zumindest hat sie das NYPD bei einer Durchsuchung eines Demonstranten bereits verwendet.

Am 07.08.2020 klopften Dutzende von New Yorker Polizeibeamten an die Tür von Derrick Ingram, einem 28-jährigen Black-Lives-Matter-Aktivisten. Ingram stand unter Verdacht einen Polizeibeamten angegriffen zu haben. Er soll ihm während einer Demonstration mit einem Megafon ins Ohr geschrien haben. Polizisten am Tatort wurden dabei gesehen, wie sie ein Dokument mit dem Titel „Facial Identification Section Informational Lead Report" (Bericht der Abteilung für Gesichtsidentifizierung) anschauten, das offenbar ein Social-Media-Foto von Ingram enthielt. Die NYPD bestätigte, dass sie bei der Suche nach Ingram die Gesichtserkennung eingesetzt hat.

Eric Adams, der neue Bürgermeister der Stadt, will den Einsatz der Gesichtserkennungs-Technologie eventuell noch erweitern. Dagegen haben sie viele US-amerikanische Städte bereits verboten, weil sie zu ungenau sei und Voreingenommenheit fördere (because of concerns about accuracy and bias). Jameson Spivack, Mitarbeiter am Georgetown Law's Center on Privacy and Technology: „Das Projekt von Amnesty zeigt auf, wie weit die Überwachung verbreitet ist, insbesondere in mehrheitlich nicht-weißen Stadtvierteln. Und es deckt auf, wie viele öffentliche Plätze gefilmt werden – Material, das die Polizei zur Gesichtserkennung einsetzen könnte" (Ryan-Mosley, New York: Kameras überwachen vor allem die üblichen Verdächtigen, www.heise.de 21.02.2022, Kurzlink: https://heise.de/-6495853).

Brasilien

Gesichtserkennungssoftware vor Gericht

Die Ombudsstelle des Bundesstaates São Paulo, deren Pendant auf Bundesebene sowie eine Gruppe zivilgesellschaftlicher Organisationen haben gemeinsam eine Klage eingereicht, um den Einsatz von Gesichtserkennungstechnologien durch die Metro in São Paulo mit ihren vier Millionen Fahrgästen täglich

zu verhindern. Ein Antrag auf Erlass einer einstweiligen Verfügung zielt darauf ab die Erfassung und Verarbeitung biometrischer personenbezogener Daten von U-Bahn-Nutzern zu unterbinden. Die Klage fordert im Hauptsacheverfahren neben der unverzüglichen Einstellung des Einsatzes von Gesichtserkennungstechnologie die Verurteilung des Unternehmens zur Zahlung einer Entschädigung in Höhe von mindestens 42 Millionen Reais (rund 7,5 Mio. Euro) für kollektive moralische Schäden für die Verletzung der Rechte seiner Fahrgäste.

Gemäß den Klägern entspricht das System nicht den Anforderungen im Allgemeinen Datenschutzgesetz, im Verbraucherschutzgesetz und weiteren Gesetzen und Verordnungen. Gemäß dem brasilianischen Datenschutzgesetz müssen bei der Verarbeitung personenbezogener Daten die Menschenrechte, die Menschenwürde und Bürgerrechte geachtet werden. Mit der Klage wird bemängelt, dass die Gesichtserkennung das Risiko der Diskriminierung schwarzer, nicht-binärer und transsexueller Menschen erhöhe, da diese Art von Technologie keine hohe Genauigkeit aufweise und „in ein Umfeld des strukturellen Rassismus eingebettet" sei. Selbst die besten Algorithmen seien bei der Erkennung von Schwarzen und Transgender-Personen ungenau, so dass diese mehr Peinlichkeiten und Rechtsverletzungen ausgesetzt wären: „In Bezug auf schwarze und transsexuelle Menschen gibt es viele öffentliche und berüchtigte Fälle im In- und Ausland, in denen Gesichtserkennungssysteme zu schwerwiegenden Fehlern geführt haben, die auf algorithmischer Diskriminierung beruhen."

Google, Amazon und andere Technologiefirmen stehen seit Jahren wegen Diskriminierung durch ihre KI-Systeme in der Kritik. Studien zeigten, dass Gesichtserkennungstechnologie farbigen Menschen gegenüber voreingenommen ist und dass Schwierigkeiten bestehen People of Color zu identifizieren. Facebooks Gesichtserkennung zum Beispiel hielt schwarze Menschen für Affen. Unschuldige Schwarze wurden aufgrund fehlerhafter Algorithmen verhaftet. Zudem verstoße, so die Klage, die Verwendung von Bildern und Daten von Kindern und Jugendlichen ohne die Zustimmung der Eltern oder Erziehungsberechtigten gegen bestehende Gesetze. Die Überwachung verletze die Privatsphäre, weshalb Länder wie die USA oder Kanada den massiven Einsatz von Gesichtserkennungstechnologie eingeschränkt haben. Im Februar 2021 hat die kanadische Datenschutzbehörde offiziell festgestellt, dass Clearviews Gesichtserkennung in Kanada illegal ist. Die US-Steuerbehörde verzichtete nach Kritik auf Gesichtserkennung für Onlinedienste.

Die Metro erwiderte, dass „die Implementierung des Systems den Anforderungen des allgemeinen Datenschutzgesetzes entspricht". Auch sehe „das elektronische Überwachungssystem (SME3) keine Gesichtserkennung des Bürgers, keine Personifizierung und keinen Aufbau einer Datenbank mit persönlichen Informationen" vor. Es diene „ausschließlich der Betriebsunterstützung und dem Passagierdienst. Damit ist es möglich Fahrgäste zu zählen, Objekte zu identifizieren, unbegleitete Kinder, unbefugtes Betreten von Bereichen wie dem Gleis, an dem der Zug vorbeifährt, entlaufene Tiere oder sehbehinderte Personen über das System zu überwachen und in diesen Situationen Warnmeldungen zu generieren, damit die Mitarbeiter schnell handeln können" (Knobloch, Brasilien: Klage gegen Gesichtserkennungssoftware, www.heise.de 08.03.2022, Kurzlink: https://heise.de/-6541767).

China

Olympiateilnehmende standen unter dauerndem Überwachungsdruck

Der US-Sicherheitsforscher Jonathan Scott hat schon vor Beginn der Olympischen Winterspiele in Beijing die für die Teilnehmer verpflichtende offizielle App My2022 dekompiliert und erhob daraufhin schwere Vorwürfe gegen China. Demnach soll die App Tonmitschnitte anfertigen: „Ich kann definitiv sagen, dass sämtliche Audioaufnahmen der Olympioniken gesammelt, analysiert und auf chinesischen Servern gespeichert werden." Scott verwies darauf, dass die chinesischen Entwickler der App auch Komponenten anderer Hersteller im Code eingebunden haben, darunter Module der chinesischen Firma iFlytek, die Audio verarbeiten können, und schloss daraus, dass die App alle eingeloggten Nutzer permanent abhört und die Daten an chinesische Server schickt. Den dekompilierten Code und die Assets der App für Android und iOS hat Scott auf Github veröffentlicht. Belege, dass die App permanent Mitschnitte anfertigt und diese weiterreicht – etwa anhand von Netzwerkverkehr – blieb Scott schuldig. Um das nachzuvollziehen, müsste man eingeloggt sein – und einen Zugang zur App erhielten nur die akkreditierten Teilnehmer der Spiele.

Zuvor hatten Sicherheitsforscher des Citizen Labs der Universität Toronto eine „einfache aber verheerende Schwachstelle" in der Verschlüsselung bei der Client-Server-Kommunikation der App gefunden. Damit konnte die Verschlüsselung, die Tonaufnahmen der Nutzer und Datentransfers schützt, mühelos umgangen werden. Laut Citizen Lab ist unklar, mit wem diese Informationen alles geteilt wurden. In Kombination seien die privaten Daten daher unzureichend geschützt. Die Analyse bestätigte, dass die Behörden mit der App theoretisch Sportler, Betreuer oder Journalisten, die sich in der Olympia-Blase aufhalten wollten oder mussten, bei den Spielen überwachen konnten, wenn sie es wollten. Während des Aufenthaltes gab es tägliche PCR-Tests und tägliches Übermitteln der Körpertemperatur.

Die Forschenden fanden in der Android-Version zudem eine Datei mit dem Namen „illegalwords.txt". Dass China in Messengerdiensten und auf Webseiten bestimmte Begriffe zensiert, war schon seit Längerem bekannt. Gemäß Citizen Lab blockierte die Chatfunktion 2442 Wörter, darunter der Name des chinesischen Staatschefs Xi Jingping oder „Tiananmen", der Name des Pekinger Platzes, auf dem das kommunistische Regime 1989 Proteste blutig niederschlug.

Auch die Sportverbände sahen die App kritisch. Der Deutsche Olympische Sportbund (DOSB) und andere nationalen Sportverbände haben den Athletinnen und Athleten empfohlen My2020 nicht auf ihrem persönlichen Gerät zu installieren. Der DOSB stellt

der deutschen Delegation dafür Sponsoren-Smartphones zur Verfügung. Beim „Team-D-Call" des DOSB hielt Thomas Biere, Referatsleiter beim Bundesamt für die Sicherheit in der Informationstechnik (BSI), eine 15-seitige PowerPoint-Präsentation und beschrieb die Risiken der App. Offiziell sollte diese den chinesischen Behörden dazu dienen, wegen der Pandemie den Gesundheitsstatus im Blick zu halten. In der App sollten die Olympioniken auch medizinische Daten wie den Impfstatus hinterlegen. Wenig vertrauensvoll war, dass die Teilnehmenden in der App bereits zwei Wochen vor der Anreise täglich ihre Körpertemperatur eintragen mussten. Biere wies darauf hin, dass die App laut Googles Play Store 44 Berechtigungen verlangt, z.B. „im Hintergrund auf den Standort zugreifen" und „Kontakte lesen". Am Eröffnungstag der Spiele war zumindest Letzteres nicht mehr in der Auflistung zu finden; aufgeführt waren noch 34 Berechtigungen.

Das BSI empfahl den Olympia-Teilnehmenden die App nur auf einem Zweithandy zu nutzen, nicht auf dem persönlichen. Es empfahl keinerlei persönliche Daten oder Chats auf dem Smartphone, auf dem My2022 läuft, zu speichern. Außerdem heißt es unter Punkt 9 der Sicherheitshinweise: „Lassen Sie Ihre Geräte nicht aus den Augen" – nicht einmal im Hotelzimmer-Safe. Für die Zeit nach der Rückkehr: „My2022 deinstallieren, Handy entsorgen". Auch Medienvertreter nutzten Wegwerfhandys und -laptops. Auch das niederländische Nationale Olympische Komitee (NOK) verteilte „saubere" Geräte, die nach der Rückkehr aus China vernichtet werden sollten.

Beim Veranstalter der Spiele, dem International Olympic Committee (IOC), sah man keine Probleme mit My2022. Die Anwendung sei ein „wichtiges Werkzeug der Anti-Covid-19-Maßnahmen". Die App sei ja nicht verpflichtend. Man könne statt der App ja auch die Web-Version von My2022 verwenden. Dies war aber wenig praktikabel, da die Teilnehmenden der Spiele mehrmals täglich Testergebnisse oder Impfzertifikate über die Plattform vorzeigen mussten. Das IOC weiter: „Der Ton wird nicht heimlich mitgeschnitten oder analysiert". Apple und Google hätten die App ja schließlich in ihren Stores freigegeben (Koopmann, Alles im Blick, SZ 05./06.02.2022, 2; Catuogno, Überwachung trifft auf Omikron, SZ 02.02.2022, 27; Knop, My 2022: Experte erhebt Spionagevorwürfe gegen Chinas Olympia-App, www.heise.de 28.01.2022, Kurzlink: https://heise.de/-6342124).

Russland

Telefonverbindungsaktion gegen Staatsführung

Mit 5.000 von Militärs, Geheimdienstlern und Politikern in Russland erbeuteten Telefonnummern startete das Kunstkollektiv „The Obfuscated Dreams of Scheherazade" (TODS) einen ambitionierten Telefonstreich unter dem Begriff „Wasterussiantime": Klickt man auf einer Website einen Button, startet eine Telefonkonferenz zwischen zwei zufällig ausgewählten Anschlüssen. Hochrangigen russischen Militärs, Geheimdienstleuten und Politikern soll es mit den Anrufen erschwert werden sich auf ihre Arbeit zu konzentrieren, so eine Pressemeldung von TODS: „Stell dir vor, du willst ein Verbrechen gegen die Menschlichkeit organisieren, aber dein Telefon hört einfach nicht auf zu klingeln!" Besondere Unruhe soll der Umstand verbreiten, dass am anderen Ende der Leitung jeweils ebenfalls ein Mitglied der russischen Führungskaste ist.

Die Leute von TODS hatten die Idee bereits am zweiten Tag des Ukrainekrieges, nachdem sie 5.000 Telefonnummern, unter anderem von Geheimdienstleuten und Duma-Mitarbeitern aus mehreren Leaks erhalten hatten. Klickt man auf der seit dem 18.05.2022 freigeschalteten Website wasterussiantime.today einen Button, startet ein „Dialer" eine Art Telefonkonferenz zwischen zwei zufällig ausgewählten Nummern aus dem Leak. Kommt die Verbindung zustande, kann man unbemerkt zuhören, wie die beiden unfreiwilligen Gesprächspartner sich gegenseitig zu erklären versuchen, was gespielt wird. Sie erfahren dabei nichts von der Identität der Person, die den Anruf von der Website gestartet hat. Es gibt auch keine Möglichkeit, zu den Russen zu sprechen.

Angesichts des russischen Überfalls auf die Ukraine halten die Kunstaktivisten ihre zweifellos illegale „interaktive Performance-Installation" für legitim, so eine TODS-Vertreterin, die sich „Neferneferuaten Myrnyy" nennt: „Wir sind militante Pazifisten. Wir wählen gewaltfreie Methoden, um gegen diesen Krieg zu kämpfen. Deshalb haben wir uns für diese zivile, friedliche Intervention entschieden." Ziel sei es Verunsicherung und Paranoia unter den Mitorganisatoren des Kriegs zu säen, so ihr Mitstreiter „Shera": „Sie werden sich fragen: Wer kennt unsere Telefonnummern? Werden wir abgehört?"

Ihre Aktion soll „für etwas Schönheit auch in dunkelsten Zeiten" sorgen und positioniert sich zwischen den Polit-Pranks des „Peng!-Kollektivs", des „Zentrums für Politische Schönheit" und dem „Hacktivism" von Gruppen wie Anonymous. Das Kollektiv besteht gemäß ironischer Selbstdarstellung aus „Artists, Scientists and Dentists", also Künstlern, Wissenschaftlern und Zahnärzten. Sie wissen aber genau, mit wem sie es hier aufnehmen. Deshalb kommunizieren sie nur mit größter Vorsicht und verstecken sich hinter Pseudonymen und erfundenen Geschichten. Wochenlang, erzählen sie, haben sie auch daran gearbeitet ihre Installation gegen Hacker zu isolieren. Ob es funktioniert hat, ob sie den erwarteten Attacken nur Stunden, ein paar Tage oder länger standhalten wird, wollten sie nicht vorhersagen (Häntzschel, Hallo? Hier spricht die Duma, SZ 19.05.2022, 1).

USA

Internetdaten bedrohen Menschen in der Abtreibungsauseinandersetzung

Mit der Eskalation der Auseinandersetzung um Abtreibung in den USA werden Daten über Schwangerschaft, Schwangerschaftsabbruch und über Meinungen dazu plötzlich gefährlich, wenn sie in falsche Hände geraten. Während der oberste Gerichtshof daran arbeitete eine Grundsatzentscheidung zum Abtreibungsrecht aufzuheben, wurde über einen Bericht des Tech-Magazins „Motherboard" bekannt, dass es bis vor Kurzem möglich

war, bei dem US-Datenhändler Safegraph Aufenthaltsinformationen zu kaufen, die Einblick darüber geben, welche Gruppen von Menschen Abtreibungskliniken besuchten. Aus den für wenige Hundert US-Dollar angebotenen Daten lässt sich schließen „woher die Besuchergruppen kamen, wie lange sie sich dort aufhielten und wohin sie anschließend gingen."

GPS-Daten sind längst nicht das einzige Mittel, um Schwangerschaften allein über das Internet eindeutig zu identifizieren und den betroffenen Nutzenden z.B. Anzeigen über Babykleidung auszuspielen. Auf Twitter berichten z.B. Frauen davon, dass sie Angst vor der weiteren Nutzung von Apps zum Zyklustracking haben, und dass sie den Ratschlag geben diese Daten schnellstmöglich zu löschen (Moostedt, Vertracktes Zyklustracking, SZ 09.05.2022, 10).

Afghanistan

Ehemalige GIZ-Mitarbeiter durch zurückgelassene Dokumente in Lebensgefahr

Die deutsche bundeseigene Entwicklungshilfeagentur Gesellschaft für Internationale Zusammenarbeit (GIZ) führte in Afghanistan ein Bildungsprojekt durch, in dem sie etwa 3.200 Afghaninnen und Afghanen beschäftigte, die Polizeikräften u.a. Lesen und Schreiben beibrachten. Anders als etwa Übersetzerinnen und Übersetzer der Bundeswehr werden die am Polizeiprojekt beteiligten Personen von der Bundesregierung im Allgemeinen nicht als Ortskräfte anerkannt und erhalten daher kein Visum für die Ausreise nach Deutschland. Presserecherchen zeigen, dass diese Menschen in großer Gefahr sind. Grund sind zahlreiche Spuren, die das GIZ-Polizeiprojekt hinterlassen hat und die die Frage aufwerfen, ob die GIZ die Daten ihrer Mitarbeitenden ausreichend geschützt hat.

Die Lehrerinnen und Lehrer mussten vor Arbeitsantritt Sicherheitsüberprüfungen durchlaufen und dies der GIZ mit Dokumenten belegen. Afghanische Sicherheitsbehörden erfassten dabei unter anderem Namen, Geburtsdaten sowie wohl auch biometrische Daten – Fingerabdrücke und Iris-Scans. Die ehemaligen GIZ-Kräfte gehen davon aus, dass diese Daten weiterhin in Polizeicomputern und Datenbanken gespeichert sind, auf die jetzt die Taliban Zugriff haben.

Betroffene berichten, dass sie aus diesem Grund keine Reisepässe beantragen. Sie fürchten, die Daten könnten sie als ehemalige GIZ-Mitarbeitende verraten. Die GIZ gab an, die Sicherheitsüberprüfungen seien von afghanischen Behörden durchgeführt worden. Die GIZ sei daran nicht beteiligt gewesen. Ob die afghanischen Behörden auch biometrische Daten aufgenommen haben, sei der GIZ nicht bekannt. Vorliegende Erkenntnisse aus solchen Sicherheitsüberprüfungen bestätigen jedoch, dass biometrische Daten erhoben wurden. E-Mails belegen, dass Mitarbeitende des Projekts der GIZ solche Dokumente übersandt haben.

Mitarbeitende mieteten zudem in mehreren afghanischen Provinzen Lagerräume an, um Bücher, Unterlagen und Lehrmaterial aufzubewahren. Viele dieser Lagerräume waren offenbar auch neun Monate nach Machtübernahme der Taliban nicht geräumt. In einigen sollen Teilnahmelisten und Dokumente über die Sicherheitsüberprüfungen lagern. Ehemalige Mitarbeitende fürchten nach eigenen Angaben um ihr Leben, falls die Räume entdeckt und die Dokumente in die Hände der Taliban gelangen sollten. Auf Facebook finden sich Fotos von Lagerräumen, die in einer Provinz offenbar von den Taliban entdeckt und ausgeräumt worden sind. Über dem Facebook-Eintrag steht, man habe zwei „versteckte Lagerhäuser" ausfindig gemacht.

Ein ehemaliger 34-jähriger Mitarbeiter der GIZ berichtet: „Wir leben in Angst. Jeden Tag, in jedem Moment." Seit der Machtübernahme der Taliban sei er mit seiner Familie auf der Flucht und verstecke sich fernab seiner Heimatprovinz. Einer seiner ehemaligen Kollegen sei getötet worden, andere seien gefoltert worden. „Wenn meine Kollegen und ich gewusst hätten, dass unsere Arbeit solche Folgen nach sich zieht, hätten wir niemals für die GIZ und Deutschland gearbeitet." Ein ehemaliger GIZ-Mitarbeiter berichtete, seit der Machtübernahme der Taliban habe er keine ruhige Nacht mehr gehabt, weil er ständig auf der Flucht ist. Deutschland habe ihn vergessen.

Die GIZ gibt an, man habe die Mitarbeitenden weder angewiesen, noch ihnen dazu geraten Räume zu mieten, um Material zu lagern. Allerdings zeigen Transportunterlagen und E-Mails, dass die GIZ Hunderte Kilogramm Bücher und Lehrmaterial an die Mitarbeitenden geliefert hat. Ein Mitarbeiter berichtet, die GIZ habe trotz Nachfragen keine Lösung für die Lagerung des Materials angeboten.

Anna-Lena Uzman hat für die Hilfsorganisation Mission Lifeline mit zahlreichen ehemaligen Mitarbeitenden des GIZ-Polizeiprojekts gesprochen: „Wir wissen, dass die Dokumente nicht in einer Art und Weise aufgehoben worden sind, wie es nach deutschen Standards angebracht gewesen wäre, sondern in Lagerhäusern, ungesichert, ungeschützt." Sie habe von ihren Kontakten Informationen über 34 dieser Lagerräume erhalten, schließt aber nicht aus, dass es noch mehr gab. Für Uzman steht außer Frage, dass ehemalige Mitarbeitende aufgrund ihrer Tätigkeit für das GIZ-Polizeiprojekt gefährdet sind: „Sie werden deshalb von den Taliban als Teil der Sicherheitskräfte betrachtet."

Das Auswärtige Amt, in dessen Auftrag die GIZ das Projekt durchführte, ließ Fragen zur Situation der ehemaligen Mitarbeitenden unbeantwortet. Das für die GIZ zuständige Bundesentwicklungsministerium gibt an, Erkenntnisse über eine systematische Verfolgung von ehemaligen Ortskräften der Entwicklungszusammenarbeit oder Werkvertragsnehmern lägen nicht vor. Dies schließe nicht aus, dass es in einzelnen Fällen zu individuellen Gefährdungen kommen könne oder gekommen sei. Für diese Menschen bestehe die Möglichkeit, eine Gefährdungsanzeige beim jeweiligen ehemaligen Arbeitgeber zu stellen.

Die Sprecherin für Fluchtpolitik der Linkspartei im Bundestag, Clara Bünger, stellte fest, dass sich die GIZ keine Gedanken gemacht hat, wie die Sicherheit der afghanischen Mitarbeiter geschützt werden könne. Sie forderte gefährdete Menschen schnell zu evakuieren: „Das Dramatische ist, dass man sehenden Auges diese Menschen alleine zurücklässt. Und da müssen wir einfach schneller handeln. Da muss mehr passieren" (Ciesielski/Zierer, Ehemalige GIZ-Mitarbeiter in Gefahr, www.tagesschau.de 17.05.2022, vgl. DANA 4/2021, 258 ff).

Rechtsprechung

EuGH

Deutsche Verbandsklage ist mit DSGVO vereinbar

Der Europäische Gerichtshof (EuGH) hat am 28.04.2022 geurteilt, dass Verbraucherschutzverbände gegen Verletzungen des Schutzes personenbezogener Daten gemäß des nationalen Rechts der EU-Mitgliedstaaten stellvertretend für Konsumenten klagen können (C-319/20). Es ist zulässig, dass ein solches gerichtliches Vorgehen unabhängig von einem Verstoß gegen das Recht einer bestimmten betroffenen Person und ohne entsprechenden Auftrag erfolgt.

Den Fall hatte der Bundesgerichtshof (BGH) dem EuGH im April 2019 vorgelegt. In dem Rechtsstreit zwischen dem Bundesverband der Verbraucherzentralen (vzbv) und der Facebook-Mutter Meta geht es darum, ob ein potenzieller Datenschutzverstoß des Betreibers eines sozialen Netzwerks auch wettbewerbsrechtliche Unterlassungsansprüche begründet und von Verbraucherschutzverbänden durch eine Klage vor den Zivilgerichten verfolgt werden kann. Der BGH hielt ein solches Vorgehen des vzbv für begründet, hegte aber Zweifel an dessen Zulässigkeit aufgrund der Stellvertreterfunktion des Verbands. Zugleich merkte der BGH an, dass vor allem die zuständigen Aufsichtsbehörden prüfen müssten, ob die Datenschutz-Grundverordnung (DSGVO) eingehalten werde.

Der EuGH stellt in dieser Rechtssache fest, dass die DSGVO einer nationalen Regelung nicht entgegensteht, nach der ein Verband zur Wahrung von Verbraucherinteressen gegen den mutmaßlichen Datenschutzverletzer eine Art Sammelklage erheben kann. Voraussetzung sei, dass es um einen Verstoß etwa gegen das Verbot der Vornahme unlauterer Geschäftspraktiken, gegen ein Verbraucherschutzgesetz oder das Gebot wirksamer Allgemeiner Geschäftsbedingungen (AGBs) gehe. Ferner müsse die betreffende Datenverarbeitung die Rechte identifizierter oder identifizierbarer natürlicher Personen aus dieser Verordnung beeinträchtigen können.

Der EuGH bestätigt, dass die DSGVO zwar grundsätzlich eine volle Rechtsharmonisierung in der gesamten EU vorsehe. Allerdings eröffnen einige Bestimmungen den Mitgliedstaaten die Möglichkeit innerhalb ihres Ermessensspielraums zusätzliche nationale Vorschriften zu erlassen. Diese dürften nur nicht „gegen den Inhalt und die Ziele dieser Verordnung verstoßen". Verbandsklagen seien an eine Reihe von Anforderungen geknüpft. Eine berechtigte Institution müsse ein im öffentlichen Interesse liegendes Ziel verfolgen, das darin besteht die Rechte der Verbraucher zu gewährleisten. Der Verband müsse den Fall zudem so einschätzen, dass seines Erachtens die Rechte einer betroffenen Person gemäß der DSGVO direkt verletzt worden sind. Es sei dagegen nicht nötig ein solches Individuum im Voraus konkret zu ermitteln. Eine solche Auslegung stehe im Einklang mit dem Ziel der DSGVO ein hohes Datenschutzniveau zu gewährleisten.

Der Gerichtshof folgte damit im Kern den Schlussanträgen des Generalanwalts Richard de la Tour, der meinte, bei der Unterlassungsklage des vzbv gegen Meta gehe es um einen potenziellen Verstoß gegen die datenschutzrechtliche Pflicht die Nutzer über Umfang und Zweck der Erhebung und Verwendung ihrer Daten zu unterrichten.

Der BGH hatte im Vorlageverfahren moniert, dass Facebook den Nutzern die erforderlichen Informationen nicht in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache übermittelt, worin der BGH, der nun sein Urteil fällen kann, einen Verstoß gegen die DSGVO sieht. In dem Verfahren geht es um das von Facebook betriebene App-Zentrum, über das kostenlos Online-Spiele anderer Anbieter zugänglich gemacht werden. Der Nutzer erteilte mit dem Button „Sofort spielen" den Betreibern der Anwendungen die Genehmigung viele seiner persönlichen Daten zu sammeln und auszuwerten. In einem Hinweis hieß es: „Durch das Anklicken von ‚Spiel spielen' oben erhält diese Anwendung: Deine allgemeinen Informationen, Deine-Mail-Adresse, Über Dich, Deine Statusmeldungen. Diese App darf in deinem Namen posten", einschließlich der Angabe des Punktestands. Der vzbv klagte, weil er diese Angaben für unzureichend hielt und darin keine wirksame Einwilligung in die Datennutzung erkennen konnte. Er sieht darin zudem einen wettbewerblichen Verstoß.

In Deutschland gibt es seit rund drei Jahren zudem das Instrument der Musterfeststellungsklage. Dabei müssen im ersten Schritt mindestens zehn, später 50 geschädigte Verbraucher mitmachen. Bekannt ist vor allem das Vorgehen von Verbraucherschützern auf Basis dieses Instruments gegen VW aufgrund der Dieselaffäre. Gewinne etwa aus Datenmissbrauch lassen sich über das Werkzeug bislang hierzulande nicht abschöpfen. Dies sehen aber neue Pläne für EU-weite Sammelklagen vor (Krempl, EuGH: Verbraucherschützer dürfen Facebook wegen Datenschutzverstoß verklagen, www.heise.de 28.04.2022, Kurzlink: https://heise.de/-7068179).

EuGH

TK-Vorratsdatenspeicherung nur unter engen Voraussetzungen

Der Gerichtshof der Europäischen Union (EuGH) hat mit Urteil vom 05.04.2022 das Verbot der Vorratsdatenspeicherung bestätigt (C-140/20) und bekräftigt, „dass das Unionsrecht einer allgemeinen und unterschiedslosen Vorratsspeicherung von Verkehrs- und Standortdaten, die elektronische Kommunikationen betreffen, zur Bekämpfung schwerer Straftaten entgegensteht". Wie schon zuvor bestätigte das Gericht, dass eine gezielte Vorrats-

speicherung für bestimmte Personenkategorien und nach einem geografischen Kriterium nach EU-Recht zulässig sein kann, ohne dass konkrete Anhaltspunkte dafür vorliegen, dass schwere Straftaten vorbereitet oder begangen werden. Das bezieht sich auf Orte oder Infrastrukturen, die regelmäßig von sehr vielen Personen aufgesucht werden, oder auf strategische Orte wie Flughäfen, Bahnhöfe, Seehäfen oder Mautstellen. Hier sei es den zuständigen Behörden möglich zur Bekämpfung schwerer Kriminalität die Anwesenheit der Personen zu ermitteln, die dort ein elektronisches Kommunikationsmittel benutzen.

In dem Verfahren ging es um einen Mann, der 2015 wegen Mordes an einer Frau in Irland zu einer lebenslangen Freiheitsstrafe verurteilt wurde. Dieser ging gegen das Urteil vor, weil seines Erachtens zu Unrecht Verkehrs- und Standortdaten verwendet wurden. Der irische High Court folgte dem Einwand, die irische Regierung legte Rechtsmittel beim Supreme Court des Landes ein, der wiederum den Fall dem EuGH zur Klärung vorlegte. Dieser stellte bei der Gelegenheit auch klar, dass nationale Gesetze dazu verpflichten können die Identität von Prepaid-SIM-Karten-Inhabern zu speichern. Dem stehe weder ein Unions-Rechtsakt noch die Datenschutzrichtlinie entgegen. Auch sei „Quick Freeze“ zulässig, aber nur zur Bekämpfung schwerer Kriminalität oder zur Verhütung der Bedrohung der nationalen Sicherheit. Bei „Quick Freeze“ werden Internetprovider erst bei einem Anfangsverdacht aufgefordert Daten zu einzelnen Teilnehmern für einen bestimmten Zeitraum zu speichern.

Der Gerichtshof weist darauf hin, nationale Gerichte seien zuständig darüber zu entscheiden, ob Beweismittel zulässig sind, die durch Vorratsdatenspeicherung gewonnen wurden. Dabei gilt laut dem Gericht, dass die Datenschutzrichtlinie für elektronische Kommunikation den Mitgliedstaaten zwar gestattet Grundrechte unter anderem zum Zweck der Bekämpfung von Straftaten zu beschränken, dabei müsse aber der Grundsatz der Verhältnismäßigkeit gewahrt werden.

Der EuGH hatte schon mit Urteil vom 08.04.2014 entschieden, dass das EU-Gesetz zur Vorratsdatenspeicherung gegen europäisches Recht verstößt und ungültig ist (C-293/12, C-594/12). Mit Urteil vom 19.10.2016 bestätigte das Gericht, dass anlasslose Vorratsdatenspeicherung illegal ist (C-582/14, DANA 4/2016, 201). Mit Urteil vom 06.10.2020 befand der Gerichtshof, Ausnahmen bei der Übermittlung und Speicherung von Verbindungsdaten seien möglich zur Bekämpfung schwerer Kriminalität oder im Fall einer Bedrohung der nationalen Sicherheit (C-511/18, C.512/18, C-520/18, DANA 4/2020, 263 ff.). Zuletzt erklärte der EuGH mit Urteil vom 02.03.2021 die estnische Vorratsdatenspeicherung für grundrechtswidrig (C-746/18, DANA 2/2021, 136). Der Druck auf den EuGH aus den EU-Mitgliedsstaaten hatte in den vergangenen Jahren zugenommen. In den mündlichen Verhandlungen wie auch hinter den Kulissen versuchten sie das Gericht von seiner grundrechtsfreundlichen Linie abzubringen mit dem Argument, Verkehrs- und Standortdaten seien für die Kriminalitätsbekämpfung unabdingbar.

Eine deutsche Regelung zur Vorratsdatenspeicherung liegt wegen eines anhaltenden Rechtsstreits seit 2017 auf Eis. Das Bundesverwaltungsgericht hatte mit Beschluss vom 25.09.2019 dazu den EuGH angerufen (6 C 12.18 u.a., DANA 4/2019, 237 f.). Einen Termin für das EuGH-Urteil in diesem Fall gibt es einem EuGH-Sprecher zufolge noch nicht. Die Ampel-Koalition will anstelle der Vorratsdatenspeicherung auf das „Quick-Freeze“-Verfahren setzen (Janisch, Anlassloses Datenspeichern bleibt tabu, SZ 06.04.2022, 5; Wilkens, EU-Gerichtshof bestätigt Verbot der Vorratsdatenspeicherung mit Ausnahmen, www.heise.de 05.04.2022, Kurzlink: https://heise.de/-6663202; EuGH betont enge Grenzen für anlasslose Datenspeicherung, www.sueddeutsche.de 05.04.2022).

TC Portugal

TK-Vorratsdatenspeicherung verfassungswidrig

Das portugiesische Verfassungsgericht, das Tribunal Constitucional (TC), hat mit Urteil vom 19.04.2022 die entscheidenden Klauseln zur Vorratsdatenspeicherung in einem nationalen Gesetz von 2008 für verfassungswidrig erklärt (Processo n.° 828/2019, ACÓRDÃO N.° 268/2022). Die für nichtig erklärten Artikel sahen vor, dass die Anbieter von Telekommunikations- und Internet-Diensten alle Verbindungs- und Standortdaten selbst bei vergeblichen Anrufversuchen für einen Zeitraum von einem Jahr speichern und zur Verhütung sowie Verfolgung schwerer Straftaten herausgeben mussten.

Das Urteil stellt fest, dass die Vorgaben „das Recht des Betroffenen auf Kontrolle und Überprüfung der Verarbeitung der ihn betreffenden Daten sowie die Wirksamkeit der verfassungsrechtlichen Garantie der Prüfung durch eine unabhängige Verwaltungsbehörde in Frage“ stellt. „Eine undifferenzierte und verallgemeinerte Verpflichtung zur Speicherung“ sämtlicher Verkehrsdaten aller Personen schränke „das Recht auf Privatsphäre und informationelle Selbstbestimmung in unverhältnismäßiger Weise ein“. Mit dem Instrument ließen sich „jederzeit Aspekte des Privat- und Familienlebens der Bürger offenbaren“. Es ermögliche es zudem „den Aufenthaltsort des Einzelnen jeden Tag und über den ganzen Tag hinweg zu verfolgen und festzustellen, mit wem er Kontakt hat, wie lange und wie regelmäßig er kommuniziert“. Die Vorratsdatenspeicherung tangiere auch Personen, bei denen kein Verdacht auf kriminelle Handlungen besteht: „Sie erfasst die elektronische Kommunikation fast der gesamten Bevölkerung, ohne jede Differenzierung, Ausnahme oder Abwägung mit dem verfolgten Ziel.“

Das Verfassungsgericht erklärte zudem einen Artikel für ungültig, wonach Betroffene nicht in jedem Fall über einen Zugriff der Ermittlungsbehörden auf die gespeicherten Daten informiert werden mussten. Ausnahmen dürften allenfalls gelten, um etwa das Leben oder die körperliche Unversehrtheit eines Dritten nicht zu gefährden. Mit den Einschränkungen sei Betroffenen „jede wirksame Kontrolle über die Rechtmäßigkeit und Ordnungsmäßigkeit dieses Zugriffs entzogen“ worden. Damit habe etwa der Anspruch auf effektiven Rechtsschutz nicht gewährleistet werden können.

Die portugiesische höchstrichterliche Entscheidung folgt auf die Grundsatzurteile des Europäischen Gerichtshofs von 2014 und 2016, in denen die Luxemburger Richter die EU-Richtlinie, die dem portugiesischen Gesetz zugrunde lag, wegen Verstoß gegen die EU-Grundrechtecharta für ungültig erklärt hatten. Damit blieben nationale Vorschriften zur Vorratsdatenspeicherung zunächst aber in Kraft. In Portugal hatte sich die Bürgerrechtsorganisation Defesa dos Direitos Digitais (D3) Ende 2017 daher an den Ombudsmann mit dem Appell gewandt die Angelegenheit vor das Verfassungsgericht zu bringen. Der Bürgerbeauftragte stimmte der Beschwerde 2019 zu und empfahl der Regierung eine Gesetzesänderung. Diese weigerte sich aber die nationalen Vorgaben mit den Grundrechten der Bürger in Einklang zu bringen. Noch im gleichen Jahr bat der Ombudsmann daher die Verfassungshüter um eine Entscheidung.

Bis zu dem nun erfolgten Urteil vergingen seit der D3-Beschwerde 32 Monate. Der Präsident der Bürgerrechtsvereinigung, Eduardo Santos, sprach daher vom „Ergebnis eines langen Weges". Endlich sei damit „die verfassungsgemäße Normalität wiederhergestellt". Die Bürger dürften nicht pauschal verdächtigt werden kriminell zu sein. Trotz der klaren EuGH-Ansagen landen Auseinandersetzungen über nationale Gesetze zum anlasslosen Protokollieren von Nutzerspuren immer wieder vor dem höchsten europäischen Gericht. Die Luxemburger Richter erklärten so jüngst etwa die Vorschriften in Belgien, Frankreich, Großbritannien und Estland für unvereinbar mit dem EU-Recht (in diesem Heft s.o.).

Das deutsche Gesetz zur mehrwöchigen Vorratsdatenspeicherung ist aufgrund von Entscheidungen von Verwaltungsgerichten ausgesetzt. Es wird vom Bundesverfassungsgericht und dem EuGH überprüft. Der Wissenschaftliche Dienst des Bundestags geht davon aus, dass die Vorgaben nicht zu halten sind. Der EuGH-Generalanwalt Manuel Campos Sánchez-Bordona hat sich in seinem Plädoyer dieser Sicht angeschlossen. Die alte schwarz-rote Bundesregierung hatte sich im Sommer bei der EU-Kommission noch gemeinsam mit anderen EU-Staaten für eine aufgebohrte Vorratsdatenspeicherung stark gemacht (Krempl, Privatsphäre: Portugiesisches Verfassungsgericht kippt Vorratsdatenspeicherung, www.heise.de 01.05.2022, Kurzlink: https://heise.de/-7070624).

BVerfG

Bayerisches Verfassungsschutzgesetz ist verfassungswidrig

Das Bundesverfassungsgericht (BVerfG) in Karlsruhe hat mit einem buchdicken Urteil vom 26.04.2022 weite Teile der im bayerischen Landesverfassungsschutzgesetz von 2016 vorgesehenen Überwachungskompetenzen für verfassungswidrig erklärt (1 BvR 1619/17). Die Befugnisse der bayerischen Verfassungsschützer bei Wohnraumüberwachung, Online-Durchsuchung, Handy-Ortung und beim Einsatz von verdeckten Mitarbeitern verstoßen gegen Grundrechte der Bürger. Geklagt hatten drei direkt betroffene Mitglieder der „Vereinigung der Verfolgten des Naziregimes – Bund der Antifaschistinnen und Antifaschisten" (VVN), die vom Verfassungsschutzamt als links-extrem eingestuft wird, auf Initiative der Gesellschaft für Freiheitsrechte (GFF).

Der Vorsitzende des Ersten Senats und Verfassungsgerichtspräsident Stephan Harbarth, der gleich zu Beginn der Urteilsverkündung klarstellte, dass dem Gericht durchaus an der Sicherheit der Republik gelegen ist, erläuterte das mit Spannung erwartete Grundsatzurteil: „Maßnahmen, die zu einer weitestgehenden Erfassung der Persönlichkeit führen können, unterliegen denselben Verhältnismäßigkeitsanforderungen wie polizeiliche Überwachungsmaßnahmen. Sonstige heimliche Überwachungsbefugnisse von Verfassungsschutzbehörden müssen hingegen nicht an das Vorliegen einer Gefahr im polizeilichen Sinne geknüpft werden." Je gewichtiger der Eingriff, desto bedeutsamer muss auch der Grund für die Überwachung sein.

Die Verfassungsrichter trennen klar zwischen polizeilicher und geheimdienstlicher Arbeit. Der Verfassungsschutz hat bei seiner ureigensten Aufgabe der Vorfeldüberwachung in der Regel größere Spielräume. Überwachungen, die tief in das Grundrecht auf freie Entfaltung, Unverletzlichkeit der Wohnung oder Unverletzlichkeit der informationstechnischen Systeme eingreifen, müssen an hohe Eingriffsschwellen, etwa einen konkreten Verdacht gegenüber dem Überwachten, gebunden bleiben. Der Inlandsgeheimdienst darf keine Superpolizei werden.

Die akustische und optische Wohnraumüberwachung muss ebenso wie die Online-Durchsuchung an die Abwehr einer konkreten Gefahr geknüpft werden. Der Geheimdienst darf dies letztlich nur subsidiär machen, wenn geeignete polizeiliche Hilfe für das bedrohte Rechtsgut ansonsten nicht rechtzeitig erlangt werden könnte.

Der bayerische Gesetzgeber, für den sich Innenminister Joachim Herrmann (CSU) in der Verhandlung im Dezember 2021 in die Bresche geworfen hatte, missachtete zudem die grundgesetzlich für Grundrechtseingriffe vorgesehenen Schutzregeln. Für den Kernbereichsschutz ist es demnach nötig, dass eine Vorabprüfung erhobener Inhalte durch eine unabhängige Stelle erfolgt. Das BVerfG meint, niemand im Verfahren habe plausibel erklären können, warum eine externe Kontrolle beim Verfassungsschutz nicht funktionieren solle.

Der Einsatz von verdeckten Mitarbeitern, der verglichen mit Wanzen im Wohnzimmer weniger gefährlich erscheinen mag, wird mit seinem Risiko beschrieben, dass „durch diese Maßnahmen eine vermeintliche Vertrauensbeziehung zunächst aufgebaut und dann ausgenutzt" wird. Solche Romeo- und Venus-Fallen können, so das Gericht „sehr schwer wiegen".

Hinsichtlich der Weitergabe der durch Verfassungsschützer gewonnenen Informationen urteilte der Senat nicht vollständig im Sinne der Beschwerdeführer. Diese hätten nicht ausreichend dargelegt, inwieweit die Übermittlung von Erkenntnissen an Stellen ins europäische Ausland oder nicht-öffentliche Stellen einen Grundrechtseingriff darstelle. Wenn die Daten nur zur Analyse genutzt werden, könnte eine Übermittlung in Ordnung sein.

Das BVerfG beanstandete, soweit die Klagen als zulässig erkannt wurden, das Fehlen klarer Regeln zu den Vor-

aussetzungen für Übermittlungen, die neben der Erhebung und Speicherung beim Verfassungsschutz einen weiteren Grundrechtseingriff darstellen. Das angegriffene Bayerische Verfassungsschutzgesetz erlaubt die Übermittlung praktisch für jeglichen Normverstoß und nicht nur beim Schutz hoher Rechtsgüter, was den verfassungsrechtlichen Ansprüchen nicht genügt.

Für nichtig und damit sofort hinfällig erklärte der Erste Senat auch die Auskunftsmöglichkeiten der Bayerischen Verfassungsschützer bei Telekommunikationsdienstleistern. Denn die betroffenen Diensteanbieter seien nach Bundesrecht nicht zur Übermittlung an das Landesamt verpflichtet oder berechtigt. Für das Nachbessern des in vieler Hinsicht verfassungswidrigen Gesetzes hat der bayerische Gesetzgeber bis zum 31. Juli 2023 Zeit.

Das BVerfG hat den Beschwerdeführern mit dem Urteil in den meisten Aspekten Recht gegeben und erzwingt so eine komplette Neufassung des bayerischen Gesetzes. Das wirkt, wie die GFF erklärte, weit über Bayern hinaus. Innenminister Herrmann bestätigte: „Es müssen wahrscheinlich der Bund und alle Länder ihre Gesetze ändern. Denn es gibt nach meiner Kenntnis kein einziges Gesetz, das all diesen Vorgaben, die heute formuliert worden sind, entspricht.“ Und auch der Mainzer Staatsrechtler Matthias Bäcker meinte, „dass das gesamte Verfassungsschutzrecht umfassend reformiert werden muss“ (Ermert, Bundesverfassungsgericht kassiert Bayerns Verfassungsschutzgesetz weitgehend, www.heise.de 26.04.2022, Kurzlink: https://heise.de/-7065975; Janisch, Die neue Bibel für den Verfassungsschutz, SZ 27.04.2022, 5; „Auswüchse beseitigen“, Der Spiegel Nr. 18 v. 20.04.2022, 11).

BVerfG

Renate Künast kann Internet-Adressen von Beleidigern einfordern

Mit Beschluss vom 19.12.2021 hat das Bundesverfassungsgericht (BVerfG) einer Beschwerde der Grünen-Politikerin Renate Künast stattgegeben, in der sie sich gegen das zivilgerichtliche Urteil zur Wehr setzte, wonach sie Beschimpfungen und sexistische Äußerungen im Internet hinnehmen müsse (Az. 1 BvR 1073/20). Wegen Verletzung ihres Persönlichkeitsrechts will die Bundestagsabgeordnete die Daten mehrerer Facebook-Nutzer erstreiten, um gerichtlich gegen die Verunglimpfungen vorgehen zu können. Zuvor hatte das Berliner Kammergericht (KG) lediglich 12 von 22 Kommentaren als strafbare Beleidigungen eingestuft und in den anderen Fällen zudem den Auskunftsanspruch verweigert. Dies beruht gemäß dem BVerfG auf einem Fehlverständnis und falschen Maßstab. Zehn Äußerungen müssen erneut geprüft werden, dabei seien die Vorgaben aus Karlsruhe zu beherzigen.

Hintergrund war ein 2016 von dem rechtsextremen Blogger Sven Liebich erstellter Facebook-Post, der Auszüge aus der Pädophilie-Debatte im Berliner Abgeordnetenhaus von 1986 enthält. Damals wurde eine Kollegin von Künast durch einen Volksvertreter der CDU gefragt, wie sie zu einem Beschluss der Grünen in Nordrhein-Westfalen (NRW) stehe, der die Strafandrohung gegen sexuelle Handlungen an Kindern aufheben wollte. Daraufhin warf Künast dazwischen: „Komma, wenn keine Gewalt im Spiel ist.“ Der Zwischenruf sollte offenkundig als Präzisierung der kolportierten Grünen-Forderung aus NRW verstanden werden. Dieses Zitat mit einem Portrait-Bild von Künast verwendete Liebich und ergänzte „ist Sex mit Kindern doch ganz o. k. Ist mal gut jetzt.“ Nachdem Künast dagegen vorging, veröffentlichte der inzwischen zu einer Freiheitsstrafe von 11 Monaten verurteilte Blogger Anfang 2019 einen Facebook-Post, erneut mit einem Porträt-Bild von Künast und dem Falschzitat. Zusätzlich beschwerte er sich über das juristische Verfahren an sich, die Aufforderung zur Unterlassung und ein in diesem Rahmen gefordertes Schmerzensgeld. In seinem Post verlinkte er auch einen Artikel der Zeitung „Welt“ zu der Pädophilie-Debatte von 1986.

Daraufhin hatten Unbekannte Künast unter anderem als „Stück Scheisse“, „altes grünes Dreckschwein“ oder „Drecks Fotze“ bezeichnet und noch drastischere und auch sexistische Posts geschrieben. Der Fall hatte für Aufsehen gesorgt, weil das Landgericht (LG) in erster Instanz entschieden hatte, dass Künast als Politikerin alle 22 Beschimpfungen hinnehmen müsse – sie habe Widerstand provoziert. Auf Künasts Beschwerde korrigierte sich das LG teilweise. Das Kammergericht (KG) hielt weitere Posts für beleidigend.

Die Karlsruher Richter beanstandeten nun die Wertung des KG zu den zehn für zulässig erachteten Posts, darunter die Formulierungen „Pädophilen-Trulla“, „Die alte hat doch einen Dachschaden, die ist hohl wie Schnittlauch man kann da nur noch“ und „Sie wollte auch mal die hellste Kerze sein, Pädodreck“. Das Gericht erläuterte dies: „Die Meinungsfreiheit wiegt umso schwerer, je mehr eine Äußerung darauf zielt, einen Beitrag zur öffentlichen Meinungsbildung zu leisten. Es wiegt umso weniger, je mehr es lediglich um die emotionalisierende Verbreitung von Stimmungen gegen einzelne Personen geht.“ Der Schutz der Meinungsfreiheit sei aus dem besonderen Schutzbedürfnis der Machtkritik erwachsen und bedeutend, schreibt das Gericht weiter. Bürgerinnen und Bürger können Amtsträgerinnen und Amtsträger anklagend und personalisiert für ihre Art der Machtausübung angreifen, „ohne befürchten zu müssen, dass die personenbezogenen Elemente solcher Äußerungen aus diesem Kontext herausgelöst werden und die Grundlage für einschneidende gerichtliche Sanktionen bilden“.

Allerdings erlaubten die Gesichtspunkte der Machtkritik nicht jede auch ins Persönliche gehende Beschimpfung von Politikerinnen und Politikern: „Gegenüber einer auf die Person abzielenden, insbesondere öffentlichen Verächtlichmachung oder Hetze setzt die Verfassung allen Personen gegenüber äußerungsrechtliche Grenzen und nimmt hiervon Personen des öffentlichen Lebens und Amtsträgerinnen und Amtsträger nicht aus.“ Auch sei bedeutend, ob eine Äußerung spontan in einer hitzigen Situation oder mit längerem Vorbedacht gefallen ist. Für die Freiheit der Meinungsäußerung wäre es besonders abträglich, wenn vor einer mündlichen Äußerung jedes Wort auf die Waagschale gelegt werden müsste. Bei schriftlichen Äußerungen sei aber ein höheres Maß an Bedacht und Zurückhaltung zu

erwarten. Dies gelte grundsätzlich auch für textliche Äußerungen in den „sozialen Netzwerken“ im Internet.

Schließlich sei auch zu bedenken, ob eine Äußerung nur an einen kleinen Personenkreis geht und ob sie nicht schriftlich gemacht wurde, meinen die Richter. Dann könnte die damit verbundene Beeinträchtigung der persönlichen Ehre geringfügiger und flüchtiger sein als im gegenteiligen Fall. Demgegenüber sei die beeinträchtigende Wirkung einer Äußerung gesteigert, wenn sie in wiederholender und anprangernder Weise, auch versehen mit Bildnissen der Betroffenen, oder besonders sichtbar in einem der allgemeinen Öffentlichkeit zugänglichen Medium getätigt wird. Ein solches Medium könne das Internet sein.

Der Schutz der Persönlichkeitsrechte von Amtsträgern und Politikern könne unter den Bedingungen der Verbreitung von Informationen durch „soziale Netzwerke“ im Internet schwerer wiegen: „Denn eine Bereitschaft zur Mitwirkung in Staat und Gesellschaft kann nur erwartet werden, wenn für diejenigen, die sich engagieren und öffentlich einbringen, ein hinreichender Schutz ihrer Persönlichkeitsrechte gewährleistet ist.“

Aufgabe der Fachgerichte ist es gemäß dem BVerfG aufgrund der Umstände des Einzelfalles die abwägungsrelevanten Gesichtspunkte herauszuarbeiten und miteinander abzuwägen. Zwar habe das Berliner KG angedeutet, dass eine Abwägung notwendig sei. Verfassungsrechtlich fehlerhaft habe es die Voraussetzungen der Beleidigung aber an die Sonderform der Schmähkritik geknüpft. Das KG hatte entschieden, die strengen Voraussetzungen, die an eine Schmähkritik und einen Wertungsexzess zu stellen seien, lägen nicht vor, weil die Kommentare noch einen hinreichenden Bezug zur Sachdebatte aufwiesen. Das BVerfG meint dazu, das KG habe die von ihm angedeutete Abwägung mit dem Persönlichkeitsrecht der Beschwerdeführerin nicht vorgenommen. Das müsse es nun nachholen.

Renate Künast nannte den Beschluss „ein Stück Rechtsgeschichte im digitalen Zeitalter“. Die Gerichte seien damit zu einer „sehr konkreten Abwägung im Einzelfall verpflichtet – und dazu auch in den sozialen Medien Zurückhaltung einzufordern“ (Koch/Wilkens, Hasskommentare: Renate Künast siegt vor dem Bundesverfassungsgericht, www.heise.de 02.02.2022, Kurzlink: https://heise.de/-6345734; Janisch, Renate Künast setzt sich durch, SZ 03.02.2022, 5).

VGH Kassel

Cookiebot mit US-Datenübermittlung darf vorläufig weiterverarbeiten

Auf Grund eines Beschlusses des Verwaltungsgerichtshofs (VGH) Kassel vom 17.01.2022 darf die staatliche Hochschule RheinMain den Dienst Cookiebot doch auf ihrer Website nutzen (Az. 10 B 2486/21). Am 01.12.2021 hatte das Verwaltungsgericht (VG) Wiesbaden der Hochschule per einstweiliger Anordnung verboten den Dienst einzusetzen (Az. 6 L 738/21, DANA 1/2022, 60 f.). Der damit verbundene Transfer von Daten in die USA sei, so das VG, rechtswidrig. Dagegen hat die Hochschule – vorerst mit Erfolg – Beschwerde eingelegt.

Die Hochschule RheinMain nutzt auf ihrer Website den Dienst Cookiebot des dänischen Anbieters Cybot, um Einwilligungen zum Setzen von Cookies einzuholen. Ein Websitebesucher, der in dem Online-Katalog der Hochschule regelmäßig nach Fachliteratur sucht, beanstandete dies und verlangte den Dienst Cookiebot nicht weiter in die Website einzubinden. Durch den Dienst werde seine IP-Adresse an einen Cloud-Anbieter mit Sitz in den USA übermittelt. Der Daten-Export in die USA sei rechtswidrig, weil die USA keinen mit EU-Standards vergleichbaren Datenschutz bieten.

Das VG gab dem Antrag statt und untersagte der Hochschule den Einsatz des Cookiebot vorläufig mittels einstweiliger Anordnung. Die Hochschule sei für die Übertragung der IP-Adressen in die USA verantwortlich, da sie die Website betreibe. Dieser Export verstoße gegen Art. 44 DSGVO. Das VG verwies darauf, dass die Hochschule keine Einwilligung der Website-Besucher für den Datenexport einhole.

Der VGH hob die einstweilige Anordnung des VG Wiesbaden auf, weil er keinen Bedarf zur Eile sah. Zudem seien die schwierigen Rechtsfragen nicht im Eilverfahren sondern in einem Hauptsacheverfahren zu beantworten. Damit darf die Hochschule den Dienst Cookiebot zunächst weiternutzen.

Dieses Verfahren hat große Bedeutung für eine Vielzahl von Websites, da viele Betreiber Cookie-Consent-Dienste oder auch andere Dienste auf ihren Websites benutzen, bei denen IP-Adressen und andere personenbezogene Daten in die USA gelangen können.

Fragen zur Nutzung von Consent-Management-Plattformen haben eine weitreichende Bedeutung und sind komplex. Der Datenexport in die USA steht auf vielen Ebenen im Fokus. Die deutschen Datenschutzbehörden haben im Dezember 2021 dazu die Orientierungshilfe Telemedien veröffentlicht und äußerten sich zu dem Export von IP-Adressen und anderen personenbezogenen Daten in die USA äußerst kritisch. Sie betonen, dass eine Einbindung solcher Dienste in Webseiten nur zulässig sei, wenn die Rechtmäßigkeit des Datenexports zuvor geprüft wurde. Damit sind die Behörden strenger als das VG Wiesbaden. Das VG hatte seine einstweilige Entscheidung wesentlich darauf gestützt, dass der Webseitenbetreiber keine Einwilligung in den Export einholt. Das Gericht war der Ansicht, die Daten hätten in die USA übermittelt werden dürfen, hätten die Website-Besucher zuvor eingewilligt. Viele Websites holen in der Praxis zusammen mit der Einwilligung in das Setzen von Cookies auch die Einwilligung zum Datenexport. Die Datenschutzbehörden halten dagegen solche Einwilligungen in den Datenexport für unwirksam, dieser sei daher rechtswidrig.

Das Landgericht (LG) München hat in einem aktuellen Urteil noch auf einen weiteren Aspekt hingewiesen. Hier ging es darum, dass ein Website-Betreiber Google Fonts nutzte und beim Aufruf der Google-Server die IP-Adressen der Website-Besucher an Google übermittelt werden. Das ist nach Ansicht des Landgerichts rechtswidrig, da es keine Rechtsgrundlage für die Übermittlung gibt. Daher hat das LG München den Betreiber der Website zu einem Schadensersatz von 100 Euro verurteilt (Az. 3

0 17493/20). Das Urteil ist noch nicht rechtskräftig. 100 Euro sind zwar nicht viel. Wenn aber alle Besucher einer Website klagen, können schnell hohe Beträge zusammenkommen (Böken, Daten in die USA: Hochschule RheinMain darf Cookiebot vorläufig weiter nutzen, www.heise.de 02.02.2022, Kurzlink: https://heise.de/-6345246).

LG München I

Kontosperrung bei Versendung von Kinderpornografie

Gemäß eines Urteils des Landgerichts München I (LG) vom 31.01.2022 darf Facebook Nutzer, die kinderpornografische Fotos verschicken, ohne Vorwarnung aussperren (Az. 42 O 4307/19). Die Richter wiesen damit die Klage eines Mannes ab, dessen Nutzerkonto Facebook im Dezember 2018 umstandslos gesperrt hatte. Der Mann hatte über den Facebook-Messengerdienst neun pornografische Mädchenfotos an einen Freund geschickt. Die von Facebook zur Ausfilterung von Pornografie eingesetzte Software erkannte die Bilder; daraufhin wurde das Konto unvermittelt gesperrt. Der Mann hatte sich zunächst bei Facebook beschwert, woraufhin das US-Unternehmen nach einer Überprüfung des Vorgangs die Kontosperrung bekräftigte. Anschließend reichte der Mann Klage ein, unter anderem mit dem Argument, dass er die Fotos nicht öffentlich, sondern nur privat verschickt hatte.

Die 42. Zivilkammer wies die Klage ab. Demnach ist Facebook bei Vorliegen eines wichtigen Grunds zur außerordentlichen Kündigung berechtigt, in Ausnahmefällen auch ohne vorherige Ankündigung. Das Verschicken von Kinderpornografie sei ein wichtiger Grund, der eine solche Ausnahme rechtfertigt. Es obliege Facebook im eigenen Unternehmensinteresse Beiträge mit strafbaren Inhalten zu löschen oder zu sperren. Der Kläger hatte argumentiert, die Kontosperrung verletze sein Recht auf Meinungsäußerung. Nach Überzeugung der Richter ist Pornografie keine Meinung (Facebook darf Nutzer aussperren, SZ 03.02.2022, 23).

Buchbesprechungen



Engelbrecht, Kai/Schwabenbauer, Thomas (Hrsg.)
Bundesmeldegesetz - Kommentar
C.H.Beck-Verlag, München 2022
ISBN 978 3 406 70222 8, 512 S., 119,00 €

(tw) So zahlreich die Literatur – und inzwischen auch die Rechtsprechung – zur DSGVO ist, so rar sind die Quellen zu vielen bereichsspezifischen Datenschutzthemen. Zu diesen Defizitsektoren gehörte bisher auch das Melderecht. Dieses trat schon 2015 in neuer Form zentralisiert als Bundesmeldegesetz in Kraft und wurde seitdem bereits 19 Mal geändert – nicht nur wegen der DSGVO, sondern zuletzt wegen der völlig neu ausgerichteten eGovernment-Strategie der früheren Bundesregierung mit dem Registermodernisierungsgesetz. Dieser Strategieansatz wird – so der neue Koalitionsvertrag – von der neuen Bundesregierung weiterverfolgt, zumal Teile des Gesetzes am 01.05.2022 in Kraft traten, bei einigen Teilen wird es ein Jahr später sein und nochmals einige – wesentliche – Teile erst, wenn die hierfür nötigen technischen Voraussetzungen geschaffen wurden. Mit der Registermodernisierung soll nun endlich ernst gemacht werden hinsichtlich einer digitalisierten Verwaltung. Zentrale Datengrundlage hierfür bleiben die kommunalen Melderegister, die aber inzwischen bundesgesetzlich einheitlich geregelt und über die geplante ID-Nummer und die Registermodernisierung zusammengeführt werden sollen.

Nach der erfolgten Regulierung kommt die Umsetzung. Für die Umsetzung bedarf es der Gesetzeskommentierung. Und diese ließ bisher zu wünschen übrig; es gab eine nicht vollständige Loseblattkommentierung, herausgegeben von Süßmuth/Laier. Die Wünsche werden nun erfüllt durch den vorliegenden Kommentar des Beck-Verlags in dessen orangener Reihe. Für einen Datenschützer werden fast alle Wünsche erfüllt. Dies liegt daran, dass die Kommentierung nicht von Ministerialbeamten erfolgt, die schon für die Ausarbeitung der Gesetzentwürfe verantwortlich waren, sondern durch DatenschützerInnen, die sich teilweise mit ihrer kritischen Sicht schon bisher einen Namen gemacht haben und die zugleich einen juristischen Blick auf die teilweise komplexe Praxis haben: Corinna Holländer, Imke Sommer, Walter Hänsle, Nils Leopold und Sven Polenz sowie als Herausgeber Kai Engelbrecht sowie der Verwaltungsrichter Thomas Schwabenbauer.

Erfreulich ist die durchgängig hohe Qualität der Erläuterungen, die sich zwar nahe am Gesetzestext orientieren, aber nicht auf die Wiedergabe der Gesetzesbegründung beschränken, sondern die Geschichte der Regelungen beleuchten – das Melderecht war schließlich in den 70ern die Mutter des Datenschutzrechts – und in die Konkretisierungen des Verordnungs- und des Landesrechts verweisen ebenso wie in die Zukunft mit den anstehenden, noch nicht in Kraft befindlichen Regeln. Bei Bedarf werden die Regelungen verfassungskritisch hinterfragt und für falsch befunden – so etwa die von Anfang an fragwürdige, inzwischen offensichtlich überholte Hotelmeldepflicht. Die Kommentierung erfolgt nicht nur aus Sicht der Betroffenen und der Meldebehörden, sondern auch mit dem Blick auf die Bedarfsträger – von den Waffenbehörden

oder der Polizei über die Werbewirtschaft und die politischen Parteien bis hin zu den Religionsgesellschaften. Die vorhandenen Quellen und die wenige verfügbare Literatur wird weitgehend – wohl nicht bis in alle Landesverästelungen und bereichsspezifischen Schnittstellen – rezipiert. Die technischen Rechtsbezüge werden erläutert, ebenso zumindest in Grundzügen die europarechtliche Basis in der DSGVO. Das Stichwortverzeichnis ist leider eher knapp und selektiv. Wer also künftig mit dem Melderecht zu tun hat, dem kann dringend empfohlen werden sich zunächst einmal im Engelbrecht/Schwabenbauer schlau zu machen.



Vogel,Paul
Künstliche Intelligenz und Datenschutz
Nomos Verlag, Baden-Baden 2022
ISBN 978-3-84876-8703-6, 262 S.

(tw) Beim Verfassen von Studien zum Datenschutz besteht ein generelles Problem: Die technische und rechtliche Entwicklung kann schneller sein als das Buch gedruckt. Erst recht gilt dies, wenn es sich bei dem Buch um eine Doktorarbeit handelt, die vor ihrer Druckveröffentlichung von zwei Promotionsgutachtern begutachtet und bewertet werden muss. Dieses Schicksal hat bei der vorliegenden Arbeit von Paul Vogel voll zugeschlagen, der sich dem hochaktuellen Thema der Künstlichen Intelligenz und dessen Datenschutzverträglichkeit aus juristischer Sicht nähert und für seine Arbeit auch noch mit dem vielversprechenden Untertitel „Vereinbarkeit intransparenter Systeme mit geltendem Datenschutzrecht und potenzielle Regulierungsansätze“ eine umfassende und zugleich zukunftsgerichtete Darstellung verspricht.

Die Promotion wurde im Wintersemester 2019/2020 angenommen. Im Vorwort wird angekündigt, dass die ausgewählte Literatur und gesetzgeberische Bestrebungen bis 2021 nachträglich berücksichtigt worden seien.

Mit Datum vom 21.04.2021, also genügend Zeit vor der Endredaktion, legte die EU-Kommission einen Verordnungsentwurf „zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz)“ vor, nachdem die EU-Verwaltung ein aufwändiges Anhörungsverfahren durchgeführt hatte, in dem aus der Praxis und der Wissenschaft viele Regulierungsanregungen einflossen, die noch nicht im Ansatz bei der Vordiskussion des Themas in der High Level-Group erkennbar waren.

Es ist nun schade, dass diese Entwicklungen in der Arbeit nur kurz dargestellt, aber nicht reflektiert werden. So halten wir ein Buch in den Händen, das – eher journalistisch – die Diskriminierungsrisiken von Künstlicher Intelligenz (KI) thematisiert, aber nicht den Bogen direkt zum Datenschutzrecht schlägt, und das es leider auch versäumt den Datenschutz bei diesem grundlegenden Thema in einen umfassenderen Kontext des digitalen Grundrechtsschutzes zu stellen. Schon gar nicht wird der risikobasierte Ansatz des Entwurfes für ein KI-Gesetz der EU nachvollzogen, geschweige denn vorgedacht, der diesen Entwurf beherrscht und der insofern in einem Gleichklang zum risikobasierten Ansatz der DSGVO steht.

Auch mit der Hoffnung dogmatisch entschädigt zu werden, wird man teilweise enttäuscht. Zwei zentrale, spannende Fragen bei KI-Nutzungen sind die nach der (gemeinsamen?) Verantwortlichkeit und die nach der Gewährleistung der Datenrichtigkeit beim Trainieren von KI, was es nötig macht KI komplex – in der zeitlichen Abfolge wie auch hinsichtlich der Beteiligten – zu beleuchten. Leider gibt es auch hierzu keine Ausführungen. Was übrig bleibt, ist eine Bearbeitung der Transparenzproblematik. Vogel geht dabei juristisch gediegen vor, indem er hohe Transparenzanforderungen ableitet und die Voraussetzungen des Art. 22 DSGVO prüft der „automatisierte Entscheidungen“ zu regulieren versucht. Nachvollziehbar begründet er dann, dass die Betroffenen ein Recht auf Information, auf Erklärung und auf menschliche Überprüfung der KI-Entscheidung haben. Aber selbst hier bleibt der Autor hinter den Erwartungen des zweifellos anspruchsvollen Rezensenten zurück. So wäre gerade der verfassungsrechtliche Anspruch des Transparenzanspruchs angesichts der digitalen Herausforderungen abzuleiten gewesen, und dann wären in einem zweiten Schritt dieser Anspruch mit konkurrierenden Grundrechten – geistiges Eigentum, Betriebs- und Geschäftsgeheimnisse – abzuschichten und zudem ins Verhältnis zu Gemeinschaftswerten (z.B. Demokratieprinzip; Schutz vor Manipulation) zu setzen gewesen. In diesem Zusammenhang wäre es dann zu erwarten, sich mit der immer noch beständigen Rechtsprechung des Bundesgerichtshofs zu Scoringverfahren als Geschäftsgeheimnisse auseinanderzusetzen. Spannend wäre auch eine Systematisierung der Risikolagen beim KI-Einsatz unter Einordnung in bestimmte Anwendungsbereiche (z.B. Medizin, Verkehr, Finanzwirtschaft).

Was nun vorliegt, ist eben eine gediegene Literaturarbeit unter Heranziehung juristischer Publikationen, die teilweise selbst unter den in der vorliegenden Rezension kritisierten Defiziten leiden. Schade: Das Thema ist vielversprechend. Vielleicht bearbeitet es in zeitlicher Nähe jemand auf aktueller Höhe und umfassend. Dabei soll nicht verschwiegen werden, dass der Stil und Form des Buchs äußerst ansprechend sind und die Quellenhinweise einen ganz guten Überblick über die Literatur bis 2019 geben. Für die Auslegung des Art. 22 DSGVO werden einige positive Erwägungen vorgetragen, so dass auch ein direkter praktischer Nutzen gezogen werden kann. Doch die Regulierungsansätze bleiben im klassischen Datenschutzniveau verhaftet und bleiben hinter den Möglichkeiten und eben auch hinter dem Entwurf eines KI-Gesetzes zurück.



Weichert, Thilo
Datenschutzrechtliche Rahmenbedingungen medizinischer Forschung
Vorgaben der EU-Datenschutz-Grundverordnung und national geltender Gesetze
Medizinisch Wissenschaftliche Verlagsgesellschaft, Berlin 2022
ISBN 9783 95466 689 8, 243 S., 59,95 €

(kjr) Im Koalitionsvertrag der Ampel wird angekündigt, dass in der 20. Legislaturperiode des Bundestags ein Forschungsdatengesetz und ein Gesundheitsdatennutzungsgesetz erarbeitet und dass eine dezentrale Forschungsdateninfrastruktur etabliert werde (vgl. DANA 1/2022, 20 f.). Hintergrund dieser Zusagen ist eine seit ca. 5 Jahren verstärkt geführte Diskussion darüber, dass die rechtlichen Grundlagen insbesondere für die medizinische Forschung in Deutschland wissenschafts- und datenschutzfeindlich seien (vgl. DANA 4/2017, 193 ff.). Den juristischen Beleg hierfür liefert nun das Buch von Weichert, das im Auftrag der „Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V.“ (TMF) verfasst und in der Schriftreihe der TMF als Band 19 veröffentlicht ist. Weichert hat sich die Aufgabe gestellt nach Änderungen des Rechts zum Patientengeheimnis und insbesondere nach Wirksamwerden der Datenschutz-Grundverordnung (DSGVO) und der nationalen Folgeregelungen den neuen rechtlichen Rahmen für medizinische Forschung zu beschreiben, um den Forschenden insofern die nötige Rechtssicherheit zu verschaffen.

Gemäß dieser Zielsetzung beschreibt das Werk zunächst die Wechselwirkung zwischen Forschungsfreiheit und Datenschutz auf Verfassungsebene und dann, wie diese in der DSGVO präzisiert wird. Dabei zeigt sich eine große Forschungsfreundlichkeit der DSGVO, die Sekundärnutzungen für wissenschaftliche Zwecke privilegiert und sogar die Betroffenenrechte im öffentlichen Forschungsinteresse einschränkt. Möglich bleibt die Legitimation wissenschaftlicher Datenverarbeitung durch die Einwilligung der Betroffenen, wobei sich aber in der Praxis erweist, dass bei langfristigen Projekten, bei Registerspeicherungen und bei offenen wissenschaftlichen Fragestellungen das Instrument der Einwilligung an praktische Grenzen stößt. Vor diesem Hintergrund erklärt sich die in der DSGVO vorgesehene auf einer Abwägung basierende Forschungsdatennutzung und die Erlaubnis, insofern auch die berufliche Schweigepflicht aufzuheben.

Relevante Rahmenbedingungen sind zudem die Neuregelung der Verantwortlichkeiten in der DSGVO, die im Forschungsbereich durch gemeinsame Verantwortlichkeiten und für Treuhändermodelle neue Perspektiven eröffnet. Der Hauptteil des Buches enthält so eine konsistente Darstellung aller rechtlichen Fragen, mit denen Medizinforschende konfrontiert werden.

Dass dies allein nicht für eine erfolgreiche medizinische Forschung genügt, hat sich anlässlich der Corona-Pandemie gezeigt. Die rechtlichen Hintergründe für das Misslingen beschreibt das abschließende Kapitel zu „Kritik und Verbesserungsmöglichkeiten“: Der forschungsfreundliche Ansatz der DSGVO wurde nicht im nationalen Recht umgesetzt. Die Forschenden sehen sich mit einem restriktiven, sich gegenseitig widersprechenden Flickenteppich von Landes- und Bundesregelungen konfrontiert, der auch nicht durch eine Berufung auf die DSGVO aufgelöst werden kann. Hier führt dann die Feststellung des gesetzlichen Novellierungsbedarfs direkt zum aktuellen Vorwort, in dem Weichert die Initiativen beschreibt, mit denen das Problem des Flickenteppichs bewältigt werden soll. Diese Initiativen münden genau darin, was die Koalitionsvereinbarung der Ampel ankündigt.

So ist das Buch zum einen eine fundierte juristisch-dogmatische Fundgrube, die sämtliche rechtlichen Streitfragen bei der Anwendung der DSGVO und des Patientengeheimnisses beantwortet, und zugleich eine an den Bundesgesetzgeber adressierte politische Streitschrift, die auf nationaler Ebene grundlegende rechtliche Änderungen einfordert. Das Buch ist auch kostenfrei im Internet zum Download verfügbar unter:

https://www.mwv-open.de/site/books/m/10.32745/9783954667000/.



Kühn, Boris/Gluns, Danielle
Vernetzte Daten, vernetzte Behörden?
Datenmanagement, Datenschutz und Kooperation in der lokalen Integrationsarbeit
Hrsg.: Robert Bosch Stiftung, Stuttgart 2022
ISBN 978 3 939574 70 5, 78 S.

(tw) Es gibt wenig Studien, in denen wissenschaftlich das Datenschutzrecht an den praktischen Bedürfnissen gemessen wird. Wohl gibt es dafür umso mehr ein interessengeleitetes Abwatschen des Datenschutzes wegen angeblicher Praxisferne. Insofern geht die vorliegende Studie, die auf das Forschungsprojekt „Hand in Hand? Chancen und Risiken des Datenmanagements in der lokalen Integrationsarbeit“ zurückgeht, einen erfreulichen Weg. Das Projekt wurde zwischen November 2020 und März 2022 von der Universität Hildesheim in Zusammenarbeit mit der Robert Bosch Stiftung GmbH durchgeführt und durch die Beauftragte der Bundesregierung für Migration, Flüchtlinge und Integration gefördert.

Die Studie bringt Licht in einen bisher wenig beleuchteten Bereich der

Datenverarbeitung zu Migranten, wo es nicht um die repressive oder rein administrative Tätigkeit der Ausländer- und Asylbehörden geht, sondern um die Unterstützung von Migranten bei deren Integration in unsere Gesellschaft durch Vermittlung von Sprach- und sonstigen Ausbildungsmöglichkeiten, von Wohnung und Arbeit. Diese wichtige Tätigkeit wird derzeit teilweise von kommunalen Stellen, teilweise von privaten und kirchlichen Einrichtungen vorgenommen. Dabei sind sie auf Daten von den Migranten angewiesen, denen zumeist nicht nur die Sprache, sondern auch die Kultur, das Vorgehen der Verwaltung sowie das Recht – einschließlich des Datenschutzrechts – fremd sind. Zur Durchführung der Studie wurden viele Gespräche mit Beteiligten der lokalen Migrations- und Integrationsarbeit sowie mit einigen Verwaltungsmitarbeitern geführt und um Erkenntnisse aus Literaturstudien ergänzt.

Die Studie zeigt große Datendefizite bei der Integrationsarbeit auf, die teilweise auf Rechtsunkenntnis, aber vorrangig auf Verwaltungsunwilligkeit und fehlende Rechtsgrundlagen zurückzuführen sind. Für eine Unterstützung der Migranten sind fast überall Identitäts- und Nachweisdokumente erforderlich; oft sind es immer wieder die selben „Papiere“, die vorgelegt werden müssen. An diese Dokumente zu gelangen, ist für die Integrationsberater oft ein zeit- und personalintensives Geschäft, da es keine vorgegebenen Strukturen, Informationswege und Abläufe gibt, mit denen die Identität der Betroffenen verbindlich festgestellt werden kann (Once only) und mit denen den administrativen Anforderungen für Nachweise genügt wird.

In Ermangelung von Alternativen helfen sich die Integrationsarbeiter oft mit Einwilligungserklärungen der Migranten, die rechtlich fragwürdig und für die Betroffenen alles andere als verständlich und transparent sind. Oft formal bestehende Möglichkeiten vom Ausländerzentralregister bis hin zu Auskunftsansprüchen gegenüber Behörden werden – nicht zuletzt wegen administrativer Abwehr – nicht genutzt. Durch die DSGVO gegebene Spielräume – im Sinne eines berechtigten oder öffentlichen Interesses – werden auch wegen den damit verbundenen Unsicherheiten nicht genutzt. Die Studie kommt zu dem Ergebnis, dass es auf verschiedenen Ebenen Verbesserungsbedarf gibt: hinsichtlich der normativen Grundlagen, der Kommunikationsschnittstellen zwischen Ausländer-, Arbeits- und Sozialbehörden sowie den Helfenden, hinsichtlich einer migrationssensiblen Dokumenteninfrastruktur und letztlich der Bereitschaft aller Beteiligten zu einem undogmatischen kreativen Vorgehen. Die Studie ist ein gutes und zugleich unschönes Beispiel dafür, wie der Datenschutz instrumentalisiert wird, um eine wichtige Aufgabe zu sabotieren oder zumindest zu behindern.

Die Studie kann im Internet heruntergeladen werden unter: https://www.bosch-stiftung.de/sites/default/files/publications/pdf/2022-03/Robert_Bosch_Stiftung_Studie_Datenmanagement_in_Integrationsarbeit.pdf oder bestellt werden bei der Robert Bosch Stiftung GmbH, Heidehofstraße 31, 70184 Stuttgart.



Heilmann, Dorothea
Recht auf Vergessenwerden
Harmonisierung eines datenschutz- und äußerungsrechtlichen Abwägungssystems im Fall von Auslistungsansprüchen
Nomos Verlag, Baden-Baden 2022
ISBN 978-3-8487-8966-5 (Print)
233 S., 65,00 €

(tw) Juristische Dissertationen, insbesondere im Datenschutzrecht, sind immer ein Wagnis: Relativ wenig praxiserfahrene Studierende am Ende des Studiums befassen sich mit einem juristischen Thema, um hierzu neue Erkenntnisse zu erlangen. Dies wagt auch Dorothee Heilmann mit ihrem hochambitionierten Titel, der Erkenntnisse zum Verhältnis Meinungsfreiheit nach Art. 5 GG bzw. Art. 11 GRCh und Persönlichkeitsrecht bzw. Datenschutz nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG bzw. Art. 8 GRCh verspricht. Das Thema ist hochrelevant, befindet sich doch die Diskussion über Fakenews und Hatespeach derzeit mit einer gewaltigen praktischen Relevanz im Hoch. Die erste Einschränkung, die man als Leser zur Kenntnis nehmen muss, ist, dass nicht das Verhältnis von Meinungsfreiheit und Persönlichkeitsrechtsschutz generell thematisiert wird, sondern nur in Bezug auf Auslistungsansprüche bei Suchmaschinen. Eine solche Beschränkung empfiehlt sich für DoktorantInnen, um sich nicht zu überheben. Beim weiteren Studium muss man aber feststellen, dass es der Autorin eigentlich nur um Google Search geht, was enttäuscht, zumal es viele weitere Suchmaschinen gibt. Auch wenn Google hier fast Monopolist ist, wäre gerade auch insofern eine differenzierende Betrachtung spannend gewesen. Dies gilt auch für die Frage der Grundrechtsbindung für private Unternehmen, wozu die Autorin – fälschlich und in Abweichung zur klaren Position des deutschen Bundesverfassungsgerichts – eine eher ablehnende Position vertritt.

Statt sich nun mit dem Phänomen Hatespeach und Fakenews empirisch zu befassen, bevor in die rechtliche Bewertung eingestiegen wird, befasst sich das Werk – bis zum Schluss – ausschließlich mit rechtsdogmatischen Erwägungen. Und diese sind leider wenig erhellend. Dies beginnt damit, dass Google beim Betrieb seiner Suchmaschine wegen des Beitrags zur Meinungsbildung einen Schutz durch die Meinungsfreiheit zugestanden bekommt. Diese – insbesondere von Google selbst – vertretene Ansicht mag im US-amerikanischen Rechtsraum zutreffen, ist aber für eine europäische Sichtweise gewagt, da die Anzeige von Suchergebnissen zunächst ausschließlich algorithmenbasiert erfolgt. Diese Algorithmen haben keine Meinungen im Blick, sondern Trafic und damit Rendite, was wirtschaftliche Grundrechte zur Anwendung bringt. Die Ansicht lässt sich allenfalls damit begründen, dass im Konfliktfall

von Google Auslistungsentscheidungen getroffen werden, bei denen aber vorrangig die Meinungsfreiheit der betroffenen Inhaltsproduzenten tangiert wird. Dass solche Auslistungen inzwischen durch sog. künstliche Intelligenz erfolgen, wäre – auch im Hinblick auf den Schutz der Meinungsfreiheit – ein spannendes Thema gewesen. Letztlich kommt dieser Frage bei der weiteren Abhandlung auch nur eine geringe Relevanz zu, zumal von der Autorin ein privilegierter Schutz als „Presse"-Suchmaschinen – korrekt – nicht zugestanden wird.

Die weitere Arbeit befasst sich ausführlich mit einer abgrenzenden Behandlung des Äußerungs- und des Datenschutzrechts statt diese von Anfang an als die beiden Seiten derselben Medaille zu behandeln. Diese abstrakten Erwägungen, die vor 10 Jahren noch Diskussionsthema sein konnten, sollten eigentlich mit der DSGVO kein Thema mehr sein, die in Art. 1 Abs. 2 erklärtermaßen einen umfassenden Ansatz des Grundrechtsschutzes verfolgt. Auch die von der Autorin durchgeführte Differenzierung zwischen Datenschutz und Schutz des allgemeinen Persönlichkeitsrechts ist im Hinblick auf Internet-Suchmaschinen eher irritierend als erhellend. Es ist dann auch wenig erstaunlich, dass das Ergebnis der ausführlichen Erörterung darin besteht, dass es eigentlich immer auf eine Grundrechtsabwägung hinausläuft – egal ob erst die Meinungsfreiheit oder erst der Datenschutz im Blick ist.

Nun wäre es spannend gewesen, die Abwägungskriterien ausführlich und systematisch erörtert zu bekommen – im Sinne eines Sphärenschutzes, des Grades der Öffentlichkeit, der Sensitivität der Daten, der Eigenbeteiligung des Betroffenen, des Beitrags zur Meinungsbildung, des sonstigen öffentlichen Interesses an der Information, an Aktualität und am Zeitablauf, an der Relevanz als Person der Zeitgeschichte, Verdachtsberichterstattung, Schmähkritik... Leider nimmt die Arbeit auch nicht diese – sich eigentlich anbietende – Kurve. Stattdessen wird – was nicht völlig irrelevant, aber eher von geringer Bedeutung ist – zwischen Wort- und Bildberichterstattung differenziert.

Wohl referiert sie ausführlich verschiedene Urteile auch europäischer und nationaler Ebene, was zweifellos verdienstvoll ist. Doch gerade eine Systematisierung wäre dringend nötig – insbesondere über die jeweiligen nationalen Unterschiede in einer EU, in der Art. 85 DSGVO mitgliedstaatsübergreifend zum Thema Meinungsfreiheit gilt. Hier ist europäische Harmonisierung angezeigt, aber keine Vollharmonisierung, zumal eben der Art. 85 DSGVO mit gutem Grund eine Öffnungsklausel enthält.

Also wäre es spannend gewesen zumindest in die Details in Deutschland einzusteigen, vom uralten Kunsturhebergesetz über Mediengesetze bis hin zum relativ neuen Netzwerkdurchsetzungsgesetz. Doch leider wieder Fehlanzeige. Fehlanzeige erst recht bzgl. des europäischen Digital Services Acts, der als Entwurf zwar erwähnt, aber inhaltlich nicht behandelt wird. So erleidet das Buch noch ein weiteres Schicksal, das bei Dissertationen weit verbreitet ist: der Verlust an Aktualität durch Zeitablauf. Es bleibt also weiteren – auch juristischen – AutorInnen vorbehalten das Spannungsverhältnis zwischen Meinungsfreiheit und Datenschutz auszuleuchten, insbesondere mit seiner inhaltlichen und seiner prozeduralen Seite – auch mit dem konkreten Bezug zu Suchmaschinen.



Dr. Kuuya Chibanguza / Christian Kuß / Hans Steege [Hrsg.]
Künstliche Intelligenz – Recht und Praxis automatisierter und autonomer Systeme
Nomos Verlagsgesellschaft, Baden-Baden 2022
ISBN 978-3-8487-7161-5

(ha) Wer dieses 1350 Seiten umfassende Werk in der Hand hält, zweifelt an dem im Vorwort formulierten Ziel einer kompakten „Gesamtdarstellung der Materie". Doch das äußerst umfangreiche Gebiet der Künstlichen Intelligenz wird in diesem Band unter vielen verschiedenen Aspekten behandelt. Den drei Herausgebern ist es zu verdanken, dass hierzu fast 80 Autorinnen und Autoren ihren Beitrag geleistet haben.

Auf die Grundlagen im ersten Teil folgt eine ausführliche Betrachtung verschiedener Branchen: von Mobilität, Gesundheit, Produktion und Handel über Arbeitsverhältnisse, Banken und Justiz bis zu Polizei, Verwaltung und Medien. Das Stichwortverzeichnis umfasst 30 Seiten und ist generell gut nutzbar. Die Auflistung des Schrifttums und weiterer Literatur zu Beginn eines jeden Kapitels hilft dagegen nur dann weiter, wenn mit einer digitalisierten Ausgabe gearbeitet wird, denn alle Angaben sind als Fließtext in einem kompletten Block gesetzt. Dasselbe Manko betrifft teils auch die Hyperlinks. So wird im Kapitel „Medizin – Gesundheit" auf Seite 602 ein Strategietext der Bundesregierung aus dem Jahr 2018 angegeben, der außer dem Namen der Website die Eingabe von über 50 Ziffern und Zeichen erfordert. Da freut es dann schon, dass die Datenschutzkonferenz (DSK) für ihre Entschließung zur Künstlichen Intelligenz mit „/media/en/20190404_hambacher-erklaerung.pdf" einen verständlichen Namen gewählt hat.

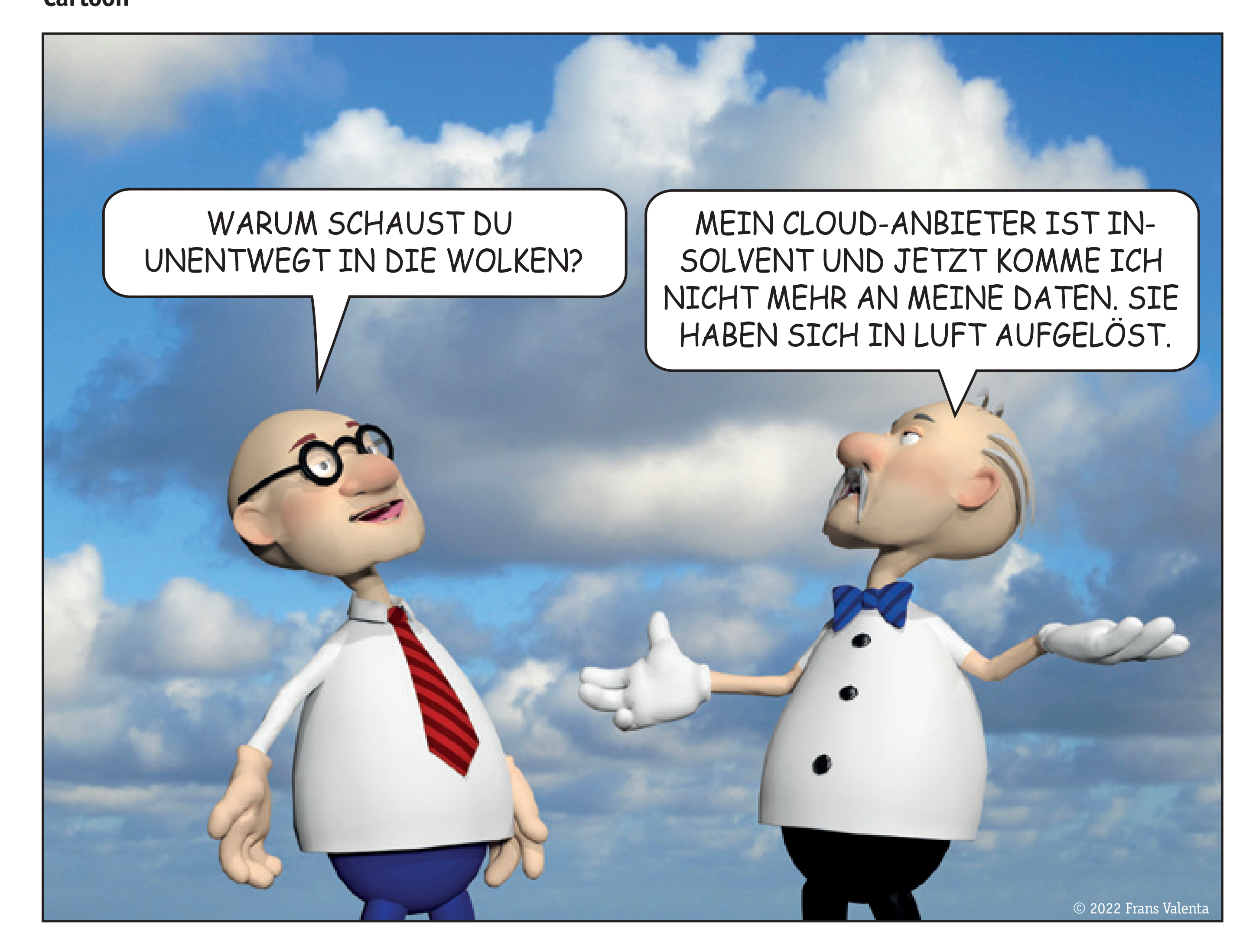
Inhaltlich tritt das Thema Datenschutz an verschiedenen Stellen auf, abhängig von der Ausrichtung der Texte mal ausführlich oder nur recht knapp umrissen. Das grundlegende Kapitel Datenschutz wird von den Herausgebern Hans Steege und Christian Kuß selbst verantwortet. Sie stellen den Status Quo nach der DSGVO dar und blicken mit Zitaten teils darüber hinaus: „Die Bedeutung des Marktortprinzips dürfte durch die Verwendung von KI zunehmen" (S. 132). So auch im Bezug auf die Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO: „Die KI birgt für den Verantwortlichen die Herausforderung, die sehr komplexen Umstände in klarer und einfacher Sprache verständlich darzustellen" (S. 139). Präzise und kritisch wird die Vertragserfüllung betrachtet, indem konstatiert wird, dass sich der Einsatz einer KI zur Optimierung von Datenverarbeitungsabläufen oder zur Verbesserung des Geschäftsmodells nicht auf Art. 6 Abs. 1 lit b stützen kann. Die klare Abhandlung der Datenschutzgrundsätze

stützt sich auf gängige Kommentare und die Hambacher Erklärung der DSK. Immer wieder wird betont, dass die Informationspflichten gegenüber der betroffenen Person „vor allem durch den komplexen Sachverhalt“ (S. 150 im Zshg. mit dem Recht auf Löschung) eine sehr große Bedeutung erhalten. Der Datenschutzbeitrag schließt ab mit dem Profiling. Dazu stellen die Autoren fest, dass es sich bei einem durch eine KI ermittelten Profiling-Ergebnis um ein personenbezogenes Datum handelt. Sie fordern deshalb im Fazit „frühzeitig das Augenmerk auf datenschutzrechtliche Implikationen zu legen“ (S. 152) und die Datenschutzbeauftragten der Unternehmen in Projekte einzubinden.

Der zweite Teil des Werkes widmet sich in zwei verschiedenen Bereichen dem Datenschutz. Hans Steege und Dr. Jutta Stender-Vorwachs betrachten im „§ 3 Verkehr und Mobilität“ das Datenschutzrecht beim automatisierten Fahren und erläutern die datenschutzrechtlichen Prinzipien Privacy by Design und Privacy by Default. Sie stellen sowohl die Probleme bei der Erprobung von Fahrzeugen als auch beim späteren Betrieb vor. Auch hier wird angeregt, dass Datenschutz „bereits bei der Konzeption des Fahrzeugs berücksichtigt werden“ soll (S. 376). Vera Jungkind und Dr. Susanne Koch beschreiben im „§ 4 Medizin – Gesundheit“ den Datenschutz im Gesundheitswesen. Sie analysieren das Datenschutzrecht einerseits im Zusammenhang mit der Generierung von KI-Anwendungen und andererseits mit deren Einsatz. Die knappe Darstellung nimmt aber keinen Bezug auf das Datenschutzkapitel. Als Fazit schließt dieser Beitrag mit sieben Hinweisen für die Praxis ab, unter anderem mit dem Schlusssatz: „Bei Verletzung datenschutzrechtlicher Vorgaben drohen empfindliche Sanktionen“ (S. 611), der insofern erwähnenswert ist, als er im Stichwortverzeichnis als einziger unter „Sanktion“ eingetragen ist.

Damit schließt sich der Kreis zum eingangs erwähnten Stichwortverzeichnis: In Bezug auf den Datenschutz befremdet es ein wenig, dass unter „Einwilligung in die Datenverarbeitung“ lediglich auf „§ 4 Medizin – Gesundheit“ verwiesen wird, während das Grundlagenkapitel von Steege und Kuß unter „Einwilligung“ mit deutlich weniger Einträgen verzeichnet ist. Sehr viel besser ist dies beim Begriff „Personenbezogene Daten“ gelöst, so dass sich beim Rezensenten ein positiver Gesamteindruck bezüglich des Datenschutzes in diesem Sammelband einstellt. Es ist anzunehmen, dass alle anderen Rechtsgebiete gleichermaßen solide behandelt werden.

Cartoon



Das Ende der Ende-zu-Ende-Verschlüsselung?



Die „Verordnung zur Festlegung von Vorschriften zur Verhütung und Bekämpfung des sexuellen Missbrauchs von Kindern" (CSA-Verordnung) der EU-Kommission zielt genau darauf ab:

Abschaffung der Privatsphäre durch Chatkontrolle

https://ec.europa.eu/home-affairs/policies/internal-security/child-sexual-abuse_en